

10/069118

PCT/JPGG/05832

日 本 国 特 許 庁

13.09.00

PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1 9 9 9 年 1 2 月 2 日

REC'D 06 NOV 2000

WIPO

PCT

出 願 番 号

Application Number:

平成 1 1 年 特 許 願 第 3 4 3 7 0 7 号

出 願 人

Applicant (s):

富士通株式会社
日本コロムビア株式会社
三洋電機株式会社

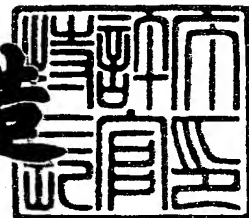
JP00105832
4

**PRIORITY
DOCUMENT**
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

2 0 0 0 年 1 0 月 2 0 日

特 許 庁 長 官
Commissioner,
Patent Office

及 川 耕 造



出 証 番 号 出 証 特 2 0 0 0 - 3 0 8 5 4 4 1

【書類名】 特許願

【整理番号】 1991489

【提出日】 平成11年12月 2日

【あて先】 特許庁長官殿

【国際特許分類】 H04M 11/08

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 畑中 正行

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 蒲田 順

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 畠山 卓久

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 長谷部 高行

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 小谷 誠剛

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 古田 茂樹

【発明者】

【住所又は居所】 東京都港区赤坂四丁目 1 4 番 1 4 号 日本コロムビア株式会社内

【氏名】 穴澤 健明

【発明者】

【住所又は居所】 大阪府守口市京阪本通 2 丁目 5 番 5 号 三洋電機株式会社内

【氏名】 日置 敏昭

【発明者】

【住所又は居所】 大阪府守口市京阪本通 2 丁目 5 番 5 号 三洋電機株式会社内

【氏名】 金森 美和

【発明者】

【住所又は居所】 大阪府守口市京阪本通 2 丁目 5 番 5 号 三洋電機株式会社内

【氏名】 堀 吉宏

【特許出願人】

【識別番号】 000005223

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号

【氏名又は名称】 富士通株式会社

【特許出願人】

【識別番号】 000004167

【住所又は居所】 東京都港区赤坂四丁目 1 4 番 1 4 号

【氏名又は名称】 日本コロムビア株式会社

【特許出願人】

【識別番号】 000001889

【住所又は居所】 大阪府守口市京阪本通 2 丁目 5 番 5 号

【氏名又は名称】 三洋電機株式会社

【代理人】

【識別番号】 100064746

【弁理士】

【氏名又は名称】 深見 久郎

【選任した代理人】

【識別番号】 100085132

【弁理士】

【氏名又は名称】 森田 俊雄

【選任した代理人】

【識別番号】 100091409

【弁理士】

【氏名又は名称】 伊藤 英彦

【選任した代理人】

【識別番号】 100096781

【弁理士】

【氏名又は名称】 堀井 豊

【先の出願に基づく優先権主張】

【出願番号】 平成11年特許願第243583号

【出願日】 平成11年 8月30日

【手数料の表示】

【予納台帳番号】 008693

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ再生装置

【特許請求の範囲】

【請求項 1】 暗号化コンテンツデータを復号してコンテンツデータの再生を行なうためのデータ再生装置であって、

前記暗号化コンテンツデータおよび前記暗号化コンテンツデータを復号するためのコンテンツキーを暗号化した暗号化コンテンツキーを格納するためのデータ格納部と、

前記データ格納部からの出力を受けて、前記暗号化コンテンツデータを再生するためのデータ再生部とを備え、

前記データ再生部は、

前記データ格納部から読み出された前記暗号化コンテンツキーを復号するための第 1 の復号鍵を保持する第 1 の鍵保持部と、

前記データ格納部からの前記暗号化コンテンツキーを基にして、前記第 1 の鍵保持部からの出力により復号処理を行なうことで、前記コンテンツキーを抽出する第 1 の復号処理部と、

前記データ格納部から読み出された前記暗号化コンテンツデータを受けて、前記第 1 の復号処理部の出力により復号してコンテンツデータを抽出するための第 2 の復号処理部を含む、データ再生装置。

【請求項 2】 前記データ再生部は、

前記データ格納部に対して前記暗号化コンテンツデータの取得のためにアクセスする毎に更新される第 1 のセッションキーを生成する第 1 のセッションキー発生部と、

前記第 1 のセッションキーを前記データ格納部にて復号可能な第 1 の暗号鍵で暗号化して前記データ格納部に与えるための第 1 の暗号化処理部と、

前記第 1 のセッションキーでさらに暗号化された上で前記データ格納部から取得した前記暗号化コンテンツキーを、前記第 1 のセッションキーについて復号して前記第 1 の復号処理部に与える第 3 の復号処理部をさらに含む、請求項 1 記載のデータ再生装置。

【請求項 3】 前記データ再生部は、前記データ格納部に対して前記暗号化コンテンツデータの取得のためにアクセスするごとに異なる第 2 のセッションキーを、さらに、前記第 1 の復号鍵により復号可能な暗号化を施して供給を受け、前記データ再生部は、

前記データ格納部に対して前記暗号化コンテンツデータの取得のためにアクセスするごとに更新される第 1 のセッションキーを生成する第 1 のセッションキー発生部と、

前記第 1 のセッションキーを、外部から入力されたデータから前記第 1 の複合鍵に基づいて前記第 1 の復号処理部にて抽出された前記第 2 のセッションキーで暗号化して前記データ格納部に与えるための第 2 の暗号処理部と、

前記第 1 のセッションキーでさらに暗号化された上で前記データ格納部から取得した前記暗号化コンテンツキーを、前記第 1 のセッションキーについて復号して前記第 1 の復号処理部に与える第 3 の復号処理部をさらに含む、請求項 1 記載のデータ再生装置。

【請求項 4】 前記コンテンツデータは、データ量を削減するための符号化方式にて符号化された符号化音楽データであって、

前記データ再生部は、

前記符号化音楽データから前記符号化方式に基づいて音楽データを再生する音楽再生部と、

再生した前記音楽データをアナログ信号に変換するデジタルアナログ変換部とをさらに含む、請求項 1 ～ 3 のいずれか 1 項に記載のデータ再生装置。

【請求項 5】 前記データ格納部は、

前記データ格納部に与えられるデータを保持するための記憶部と、

前記第 1 の暗号化鍵を保持する第 2 の鍵保持部と、

前記第 1 の暗号化鍵により暗号化されたデータを復号するための第 2 の復号鍵を保持するための第 3 の鍵保持部と、

前記第 2 の復号鍵に基づいて、前記データ再生部から前記第 1 の暗号化鍵により暗号化されて伝達された前記第 1 のセッションキーを復号するための第 4 の復号処理部と、

前記第 4 の復号処理部で抽出された前記第 1 のセッションキーにより、前記記憶部に保持されたデータを暗号化して出力するための第 2 の暗号化処理部を備える、請求項 2 記載のデータ再生装置。

【請求項 6】 前記データ格納部は、

前記データ格納部に与えられるデータを保持するための記録部と、

前記暗号化コンテンツデータを取得のためにアクセスされるごとに更新する第 2 のセッションキーを発生する第 2 のセッションキー発生部と、

前記第 1 の復号鍵にて復号可能な第 2 の暗号化鍵により、暗号化処理を行なう第 3 の暗号化処理部と、

前記第 2 のセッションキーに基づいて、前記データ再生部から前記第 2 のセッションキーにて暗号化されて伝達された前記第 1 のセッションキーを復号するための第 5 の復号処理手段と、

前記第 5 の復号処理手段にて抽出された前記第 1 のセッションキーにより、前記記憶部に保持されたデータを暗号化して出力するための第 4 の暗号化処理部を備える、請求項 3 記載のデータ再生装置。

【請求項 7】 前記データ格納部は、前記データ再生部に対して着脱可能なメモリカードである、請求項 5 または 6 記載のデータ再生装置。

【請求項 8】 前記データ再生部は、

少なくとも前記第 1 の鍵保持部と、前記第 1 の復号処理部と、前記第 2 の復号処理部とが、第三者には読出不可能なセキュリティ領域に設けられている、請求項 1 記載のデータ再生装置。

【請求項 9】 前記データ再生部は、第三者には読出不可能なセキュリティ領域に設けられる、請求項 1 ～ 4 のいずれか 1 項に記載のデータ再生装置。

【請求項 10】 暗号化コンテンツデータを復号してコンテンツデータの再生を行なうためのデータ再生装置であって、

前記暗号化コンテンツデータおよび前記暗号化コンテンツデータを復号するためのコンテンツキーを保持し、かつ、前記データ再生装置に着脱可能なデータ格納部と、

前記データ格納部からの出力を受けて、前記暗号化コンテンツデータを再生す

るためのデータ再生部とを備え、

前記データ再生部は、

前記データ格納部から読み出された前記暗号化コンテンツデータを受けて、復号してコンテンツデータを抽出するための第 1 の復号処理部と、

認証データを認証鍵により復号可能な暗号化を施して保持し前記データ格納部に対して出力可能な認証データ保持部とを含み、

前記データ格納部は、

前記認証鍵により暗号化されて前記データ再生部から与えられる前記認証データを復号して抽出するための第 2 の復号処理部と、

前記第 2 の復号処理部により抽出された前記認証データに基づいて認証処理を行う制御手段とを含む、データ再生装置。

【請求項 1 1】 前記データ再生部は、

前記データ格納部に対して前記暗号化コンテンツキーの取得のためにアクセスする毎に更新されるセッションキーを生成するセッションキー発生部と、

前記セッションキーを前記データ格納部にて復号可能な第 1 の暗号鍵で暗号化して前記データ格納部に与えるための暗号化処理部と、

前記第 1 のセッションキーで暗号化されて前記データ格納部から受信した前記コンテンツキーを、前記第 1 のセッションキーについて復号する第 3 の復号処理部をさらに含む、請求項 1 0 記載のデータ再生装置。

【請求項 1 2】 前記認証データ保持部は、第 1 の復号鍵で復号可能な暗号化を施す第 2 の暗号鍵を前記認証データとともに前記認証鍵により復号可能な暗号化を施して保持し、前記データ格納部に対して出力し、

前記第 3 の復号処理部は、前記第 2 の暗号鍵で暗号化された上で前記データ格納部から受信した前記第 1 の暗号化鍵を、前記第 1 の復号鍵にて復号し、前記暗号化処理部に与える第 4 の復号処理部を備える、請求項 1 1 記載のデータ再生装置。

【請求項 1 3】 前記第 4 の復号処理部は、さらに、

前記第 1 の復号鍵で復号可能な第 2 の暗号鍵で暗号化され、さらに前記セッションキーで暗号化された上で前記データ格納部から受信した前記コンテンツキー

を、前記第3の復号処理部にて前記セッションキーについて復号し、得られた前記第2の暗号化鍵にて暗号化された前記コンテンツキーを入力として、前記第1の復号鍵にて復号し、前記第1の復号処理部に与える、請求項11記載のデータ再生装置。

【請求項14】 前記データ再生部は、

さらに、予め定められた第2復号鍵にて復号する第5の復号処理部を備え、
前記第5の復号処理部は、

前記第4の復号鍵で復号可能な暗号化を施されて、さらに前記セッションキーで暗号化された上で前記データ格納部から受信した前記コンテンツキーを、前記第3の復号部にて前記セッションキーについて復号し、得られた第4の復号鍵で復号可能な暗号化を施された前記コンテンツキーを入力とし、

前記第2の復号鍵にて復号し、前記第1の復号処理部に与える、請求項11または12記載のデータ再生装置。

【請求項15】 前記データ格納部は、前記データ再生部に対して着脱可能なメモリカードである、請求項10～14のいずれか1項に記載のデータ再生装置。

【請求項16】 前記データ再生装置は、さらに、簡易携帯電話網を含む携帯電話網に接続するインタフェースを備える、請求項10～14のいずれか1項に記載のデータ再生装置。

【請求項17】 前記データ再生装置は、さらに、前記インタフェースを介して通話を行なう通話処理部を備える、請求項16記載のデータ再生装置。

【請求項18】 前記データ格納部は、前記データ再生部に対して着脱可能である、請求項17に記載のデータ再生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、携帯電話網等のデータ配信システムにより配送された配信データの再生装置に関し、より特定的には、配信されたデータに対する著作権保護を可能とするデータ再生装置に関するものである。

【 0 0 0 2 】

【従来の技術】

近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【 0 0 0 3 】

このような情報通信においてはデジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽データや画像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【 0 0 0 4 】

したがって、このような情報通信網上において、音楽データや画像データ等の著作権の存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【 0 0 0 5 】

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物の複製に際して一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【 0 0 0 6 】

【発明が解決しようとする課題】

ところで、上述したようなデジタル情報通信網を介した音楽データなどの著作権データの配信が行なわれた場合、各ユーザは、このようにして配信されたデータを何らかの記録装置に記録した上で、再生装置で再生することになる。

【 0 0 0 7 】

このような記録装置としては、たとえば、メモ리카ードのように電氣的にデータの書込および消去が可能な媒体が用いられることになる。

【 0 0 0 8 】

さらに、配信データを再生する装置としては、このようなデータの配信を受けるのに用いた携帯電話機自身を用いる場合や、あるいは、記録装置がメモリカードなどのように配信を受ける装置から着脱可能な場合は、専用の再生装置を用いることも可能である。

【0009】

この場合、著作権者の権利保護のためには、著作権者の承諾なしに、このようにして配信を受けたコンテンツデータ（音楽データ等）を自由に当該記録媒体から他の記録媒体等へ移転できないように記録媒体においてセキュリティ対策を施す必要がある。

【0010】

そのみならず、このようにして正当な対価を支払った上でコンテンツデータの配信を受けたユーザ以外のものが、当該記録媒体から音楽データ等の再生を行なう際に、再生装置側においてコンテンツデータを外部から自由に読み出すことができる」とすると、著作権者の権利保護ならびに正規のユーザ側の権利保護にも支障を来すことになる。

【0011】

本発明は、上記のような問題点を解決するためになされたものであって、その目的は、配信されて記録装置に保持された音楽データ等の著作物データを再生する再生装置において、ユーザ以外の者が無断で当該著作物データに対してアクセスを行なうことから保護する機能を備えたデータ再生装置を提供することである。

【0012】

【課題を解決するための手段】

請求項1記載のデータ再生装置は、暗号化コンテンツデータを復号してコンテンツデータの再生を行なうためのデータ再生装置であって、暗号化コンテンツデータおよび暗号化コンテンツデータを復号するためのコンテンツキーを暗号化した暗号化コンテンツキーを格納するためのデータ格納部と、データ格納部からの出力を受けて、暗号化コンテンツデータを再生するためのデータ再生部とを備え、データ再生部は、データ格納部から読み出された暗号化コンテンツキーを復号

するための第1の復号鍵を保持する第1の鍵保持部と、データ格納部からの暗号化コンテンツキーを基にして、第1の鍵保持部からの出力により復号処理を行なうことで、コンテンツキーを抽出する第1の復号処理部と、データ格納部から読み出された暗号化コンテンツデータを受けて、第1の復号処理部の出力により復号してコンテンツデータを抽出するための第2の復号処理部を含む。

【0013】

請求項2記載のデータ再生装置は、請求項1記載のデータ再生装置の構成に加えて、データ再生部は、データ格納部に対して暗号化コンテンツデータの取得のためにアクセスする毎に更新される第1のセッションキーを生成する第1のセッションキー発生部と、第1のセッションキーをデータ格納部に復号可能な第1の暗号鍵で暗号化してデータ格納部に与えるための第1の暗号化処理部と、第1のセッションキーでさらに暗号化された上でデータ格納部から取得した暗号化コンテンツキーを、第1のセッションキーについて復号して第1の復号処理部に与える第3の復号処理部をさらに含む。

【0014】

請求項3記載のデータ再生装置は、請求項1記載のデータ再生装置の構成に加えて、データ再生部は、データ格納部に対して暗号化コンテンツデータの取得のためにアクセスするごとに異なる第2のセッションキーを、さらに、第1の復号鍵により復号可能な暗号化を施して供給を受け、データ再生部は、データ格納部に対して暗号化コンテンツデータの取得のためにアクセスするごとに更新される第1のセッションキーを生成する第1のセッションキー発生部と、第1のセッションキーを、外部から入力されたデータから第1の複合鍵に基づいて第1の復号処理部にて抽出された第2のセッションキーで暗号化してデータ格納部に与えるための第2の暗号処理部と、第1のセッションキーでさらに暗号化された上でデータ格納部から取得した暗号化コンテンツキーを、第1のセッションキーについて復号して第1の復号処理部に与える第3の復号処理部をさらに含む。

【0015】

請求項4記載のデータ再生装置は、請求項1～3のいずれか1項に記載のデータ再生装置の構成に加えて、コンテンツデータは、データ量を削減するための符

号化方式にて符号化された符号化音楽データであって、データ再生部は、符号化音楽データから符号化方式に基づいて音楽データを再生する音楽再生部と、再生した音楽データをアナログ信号に変換するデジタルアナログ変換部とをさらに含む。

【0016】

請求項5記載のデータ再生装置は、請求項2記載のデータ再生装置の構成に加えて、データ格納部は、データ格納部に与えられるデータを保持するための記憶部と、第1の暗号化鍵を保持する第2の鍵保持部と、第1の暗号化鍵により暗号化されたデータを復号するための第2の復号鍵を保持するための第3の鍵保持部と、第2の復号鍵に基づいて、データ再生部から第1の暗号化鍵により暗号化されて伝達された第1のセッションキーを復号するための第4の復号処理部と、第4の復号処理部で抽出された第1のセッションキーにより、記憶部に保持されたデータを暗号化して出力するための第2の暗号化処理部を備える。

【0017】

請求項6記載のデータ再生装置は、請求項3記載のデータ再生装置の構成に加えて、データ格納部は、データ格納部に与えられるデータを保持するための記録部と、暗号化コンテンツデータを取得のためにアクセスされるごとに更新する第2のセッションキーを発生する第2のセッションキー発生部と、第1の復号鍵にて復号可能な第2の暗号化鍵により、暗号化処理を行なう第3の暗号化処理部と、第2のセッションキーに基づいて、データ再生部から第2のセッションキーにて暗号化されて伝達された第1のセッションキーを復号するための第5の復号処理手段と、第5の復号処理手段にて抽出された第1のセッションキーにより、記憶部に保持されたデータを暗号化して出力するための第4の暗号化処理部を備える。

【0018】

請求項7記載のデータ再生装置は、請求項5または6記載のデータ再生装置の構成に加えて、データ格納部は、データ再生部に対して着脱可能なメモリカードである。

【0019】

請求項 8 記載のデータ再生装置は、請求項 1 記載のデータ再生装置の構成に加えて、データ再生部は、少なくとも第 1 の鍵保持部と、第 1 の復号処理部と、第 2 の復号処理部とが、第三者には読出不可能なセキュリティ領域に設けられている。

【0020】

請求項 9 記載のデータ再生装置は、請求項 1～4 のいずれか 1 項に記載のデータ再生装置の構成に加えて、データ再生部は、第三者には読出不可能なセキュリティ領域に設けられる。

【0021】

請求項 10 記載のデータ再生装置は、暗号化コンテンツデータを復号してコンテンツデータの再生を行なうためのデータ再生装置であって、暗号化コンテンツデータおよび暗号化コンテンツデータを復号するためのコンテンツキーを保持し、かつ、データ再生装置に着脱可能なデータ格納部と、データ格納部からの出力を受けて、暗号化コンテンツデータを再生するためのデータ再生部とを備え、データ再生部は、データ格納部から読み出された暗号化コンテンツデータを受けて、復号してコンテンツデータを抽出するための第 1 の復号処理部と、認証データを認証鍵により復号可能な暗号化を施して保持しデータ格納部に対して出力可能な認証データ保持部とを含み、データ格納部は、認証鍵により暗号化されてデータ再生部から与えられる認証データを復号して抽出するための第 2 の復号処理部と、第 2 の復号処理部により抽出された認証データに基づいて認証処理を行う制御手段とを含む。

【0022】

請求項 11 記載のデータ再生装置は、請求項 10 記載のデータ再生装置の構成に加えて、データ再生部は、データ格納部に対して暗号化コンテンツキーの取得のためにアクセスする毎に更新されるセッションキーを生成するセッションキー発生部と、セッションキーをデータ格納部にて復号可能な第 1 の暗号鍵で暗号化してデータ格納部に与えるための暗号化処理部と、第 1 のセッションキーで暗号化されてデータ格納部から受信したコンテンツキーを、第 1 のセッションキーについて復号する第 3 の復号処理部をさらに含む。

【0023】

請求項12記載のデータ再生装置は、請求項11記載のデータ再生装置の構成に加えて、認証データ保持部は、第1の復号鍵で復号可能な暗号化を施す第2の暗号鍵を認証データとともに認証鍵により復号可能な暗号化を施して保持し、データ格納部に対して出力し、第3の復号処理部は、第2の暗号鍵で暗号化された上でデータ格納部から受信した第1の暗号化鍵を、第1の復号鍵にて復号し、暗号化処理部に与える第4の復号処理部を備える。

【0024】

請求項13記載のデータ再生装置は、請求項11記載のデータ再生装置の構成に加えて、第4の復号処理部は、さらに、第1の復号鍵で復号可能な第2の暗号鍵で暗号化され、さらにセッションキーで暗号化された上でデータ格納部から受信したコンテンツキーを、第3の復号処理部にてセッションキーについて復号し、得られた第2の暗号化鍵にて暗号化されたコンテンツキーを入力として、第1の復号鍵にて復号し、第1の復号処理部に与える。

【0025】

請求項14記載のデータ再生装置は、請求項11または12記載のデータ再生装置の構成に加えて、データ再生部は、さらに、予め定められた第2復号鍵にて復号する第5の復号処理部を備え、第5の復号処理部は、第4の復号鍵で復号可能な暗号化を施されて、さらにセッションキーで暗号化された上でデータ格納部から受信したコンテンツキーを、第3の復号部にてセッションキーについて復号し、得られた第4の復号鍵で復号可能な暗号化を施されたコンテンツキーを入力とし、第2の復号鍵にて復号し、第1の復号処理部に与える。

【0026】

請求項15記載のデータ再生装置は、請求項10～14のいずれか1項に記載のデータ再生装置の構成に加えて、データ格納部は、データ再生部に対して着脱可能なメモリカードである。

【0027】

請求項16記載のデータ再生装置は、請求項10～14のいずれか1項に記載のデータ再生装置の構成に加えて、データ再生装置は、さらに、簡易携帯電話網

を含む携帯電話網に接続するインタフェースを備える。

【0028】

請求項 17 記載のデータ再生装置は、請求項 16 記載のデータ再生装置の構成に加えて、データ再生装置は、さらに、インタフェースを介して通話を行なう通話処理部を備える。

【0029】

請求項 18 記載のデータ再生装置は、請求項 17 記載のデータ再生装置の構成に加えて、データ格納部は、データ再生部に対して着脱可能である。

【0030】

【発明の実施の形態】

〔実施の形態 1〕

〔システムの全体構成〕

図 1 は、本発明の情報配信システムの全体構成を概略的に説明するための概念図である。

【0031】

なお、以下では携帯電話網を介して、暗号化された音楽データを各ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、暗号化された他の著作物情報データ、例えば画像データ等の著作物情報データを、復号して平文化して再生することが可能なものである。

【0032】

なお、ここで携帯電話網としては、PHS (Personal Handy Phone) などの簡易携帯電話網も含むものとする。

【0033】

図 1 を参照して、著作権の存在する音楽データを管理する配信サーバ 10 は、所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化したうえで、情報を配信するための配信キャリア 20 である携帯電話会社に、このような暗号化データを与える。

【0034】

配信キャリア 20 は、自己の携帯電話網を通じて、各ユーザからの配信要求（配信リクエスト）を配信サーバ 10 に中継する。配信サーバ 10 は、配信リクエストがあると、要求された暗号化音楽情報を携帯電話会社 20 の携帯電話網を介して、各ユーザの携帯電話機に対してコンテンツデータを配信する。

【0035】

さらに、たとえばユーザ 1 は、携帯電話機 100 に接続したヘッドホン 140 等を介してこのような再生された音楽データを聴取することが可能である。

【0036】

以下では、このような配信サーバ 10 と配信キャリア（携帯電話会社）20 とを併せて、音楽サーバ 30 と総称することにする。

【0037】

また、このような音楽サーバ 30 から、各携帯電話端末等に音楽情報を伝送する処理を「配信」と称することとする。

【0038】

しかも、配信キャリア 20 において、たとえば 1 曲分の音楽データを配信するたびにその度数を計数しておくことで、ユーザが著作物データを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア 20 が携帯電話機の通話料金として徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【0039】

しかも、このような著作物データの配信は、携帯電話網というクローズドなシステムを介して行なわれるため、インターネット等のオープンなシステムに比べて、著作権保護の対策を講じやすいという利点がある。

【0040】

〔配信サーバ 10 の構成〕

図 1 において配信サーバ 10 は、音楽データ（コンテンツデータ）を所定の方法に従って暗号化したコンテンツデータやコンテンツキー等の配信情報を保持するための配信情報データベース 304 と、各ユーザごとに音楽情報へのアクセス回数等に従った課金情報を保持するための課金データベース 302 と、暗号化コ

コンテンツデータを復号するためのコンテンツキーK_cを公開暗号化鍵K_{Pp}により暗号化するためのコンテンツキー暗号化処理部316と、配信情報データベース304および課金データベース302とデータバスBS1を介してデータ授受を行ない、配信サーバ10の動作を制御するためのコントローラ312と、通信網を介して、配信サーバ10と配信キャリア20との間でデータ授受を行なうための通信装置350とを備える。

【0041】

すなわち、配信情報データベース304からは、コンテンツデータD_cが、復号鍵であるコンテンツキーK_cにより復号可能な状態に暗号化された暗号化コンテンツデータ[D_c]K_cと、コンテンツキーK_cとが出力される。コントローラ312は、コンテンツキー暗号化処理部316を制御して、このコンテンツキーK_cを公開暗号化鍵K_{Pp}により暗号化した[K_c]K_pを通信装置350を介して、配信キャリア20に与える。

【0042】

ここで、[Y]Xという表記は、データYを、キー(鍵)Xにより復号可能な暗号に変換したデータであることを示している。なお、暗号化処理、復号処理で用いられる鍵を、「キー」とも称することとする。

【0043】

〔端末(携帯電話機)の構成〕

図2は、図1に示した携帯電話機100の構成を説明するための概略ブロック図である。

【0044】

携帯電話機100は、携帯電話網により無線伝送される信号を受信するためのアンテナ1102と、アンテナ1102からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ1102に与えるための送受信部1104と、携帯電話機100の各部のデータ授受を行なうためのデータバスBS2と、データバスBS2を介して携帯電話機100の動作を制御するためのコントローラ1106と、外部からの指示を携帯電話機100に与えるためのタッチキーやダイヤルキーなどを含むキーボード1108と、コント

ローラ 1106 等から出力される情報をユーザに視覚情報として与えるためのディスプレイ 1110 と、通常の通話動作において、データバス BS2 を介して与えられる受信データに基づいて音声を再生するための音声再生部 1112 とを備える。

【0045】

携帯電話機 100 は、さらに、サーバ 30 からの暗号化コンテンツデータ [Dc] Kc および暗号化コンテンツキー [Kc] Kp を格納するためのメモリ 110 と、音楽再生モジュール 1500 とを備える。この音楽再生モジュール 1500 は、公開暗号化鍵 KPp に対応し、キー KPp で暗号化されたデータを復号可能な秘密復号鍵 Kp を保持する Kp 保持部 1540 と、音楽サーバ 30 から伝送され公開暗号化鍵 KPp により暗号化コンテンツキー [Kc] Kp をメモリ 110 から受けて復号するための復号処理部 1530 と、音楽サーバ 30 から配信されメモリ 110 中に格納された暗号化コンテンツデータ [Dc] Kc を、復号処理部 1530 で復号抽出されたコンテンツキー Kc に基づいて復号するための復号処理部 1520 と、復号処理部 1520 からの復号されたコンテンツデータを受けて、コンテンツデータを符号化した符号化方式、例えば MP3、AC3 等のデジタル圧縮符号化方式の再生手順に従って音楽データを再生するための音楽再生部 1508 と、音楽再生部 1508 の出力と音声再生部 1112 の出力とを受けて、動作モードに応じて選択的に出力、または、両者を混合して出力するための混合部 1510 と、混合部 1510 の出力を受けて、外部に出力するためのアナログ信号に変換するデジタルアナログ変換部 1512 とを含む。

【0046】

携帯電話機 100 は、さらに、デジタルアナログ変換部 1512 の出力を受けて、ヘッドホン 140 と接続するための接続端子 1514 とを含む。

【0047】

なお、説明の簡素化のため本発明の音楽データの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

【0048】

また、図2に示した構成において、音楽再生部1508、Kp保持部1540、復号処理部1530および復号処理部1520を、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールTRMに組み込む構成とすることが可能である。このようなモジュールは、一般にはタンパーレジスタンスモジュール (Tamper Resistance Module) と呼ばれる。

【0049】

このような構成とすることで、すくなくとも、復号鍵および平文化されたデータを外部から参照できないため、携帯電話機100の暗号化方式および秘密復号鍵を外部から不正に取得することが困難となり、セキュリティが向上する。

【0050】

さらに、図2において実線で囲んだ領域に相当する音楽再生モジュール1500を、TRMとすることも可能である。このような構成とすれば、音楽データ等の著作権の存在するデータの最終的なデジタルデータについても、保護することが可能である。

【0051】

[再生処理]

図3は、携帯電話機100内において、メモリ110に保持された暗号化コンテンツデータから、コンテンツデータを復号して、音楽として外部に出力するための再生処理を説明するフローチャートである。

【0052】

図3を参照して、携帯電話のキーボード1108等からのユーザの指示により、再生リクエストがコントローラ1106に与えられる (ステップS100)。

【0053】

この再生リクエストに応じて、コントローラ1106は、メモリ110を制御して暗号化コンテンツキー [Kc] Kpを読み出す (ステップS102)。

【0054】

つづいて、復号処理部1530は、メモリ110から読み出された暗号化コン

テンツキー [Kc] Kp に対する復号処理を行なう (ステップ S104)。

【0055】

復号処理部 1530 においてコンテンツキー Kc を復号抽出可能な場合は (ステップ S106)、処理は次のステップに移行し、一方、復号不能と判断された場合は、処理は終了する (ステップ S110)。

【0056】

復号処理部 1530 においてコンテンツキー Kc を復号抽出可能な場合は、コントローラ 1108 は、メモリ 110 を制御して、暗号化コンテンツデータ [Dc] Kc を読み出して、復号処理部 1520 に与え、復号処理部 1520 は、復号鍵 Kc により復号処理して、平文化したコンテンツデータ Dc を生成して音楽再生部 1508 に与える。音楽再生部 1508 においてコンテンツデータ Dc より再生された音楽信号は、混合部 1510 を経由して、デジタルアナログ変換器 1512 によりアナログ信号に変換されて接続端子 1514 から外部に出力される。

【0057】

以上のような構成とすることで、再生装置である携帯電話機 100 内のメモリ 110 には、暗号化コンテンツデータと暗号化コンテンツキーが保持されているのみであるため、外部からこのメモリ 110 内の記憶内容を仮に読み出したとしても、音楽を再生することはできない。

【0058】

しかも、メモリ 110 から復号処理部 1520 および 1530 に与えられるデータも、このような暗号化されたデータであるため、データバス BS2 上の信号を外部から仮に検出したとしても、音楽を再生することはできない。

【0059】

さらに、平文化された音楽データが伝達される部分は、上述のとおり、タンパレージスタンスモジュールで構成されているので、この部分から音楽データを外部に読み出すこともできない構成となっている。

【0060】

したがって、図 2 に示した携帯電話機 100 の構成により、不正な手続きでコ

ンテンツデータを複製して、再生あるいは配布を行なうことから保護することが可能となる。

【 0 0 6 1 】

〔実施の形態 2〕

図 4 は、本発明の実施の形態 2 の携帯電話機 2 0 0 の構成を説明するための概略ブロック図であり、実施の形態 1 の図 2 と対比される図である。

【 0 0 6 2 】

図 2 に示した携帯電話機 1 0 0 の構成と、携帯電話機 2 0 0 の構成が異なる点は、以下のとおりである。

【 0 0 6 3 】

まず、図 4 においては、携帯電話機 2 0 0 には、携帯電話機 2 0 0 により受信された暗号化コンテンツデータを受取って格納し、暗号化コンテンツデータおよび暗号化コンテンツキーをさらに所定の暗号化処理をした上で、携帯電話機 2 0 0 中の音楽再生モジュール 1 5 0 0 に与えるための着脱可能なメモリカード 1 2 0 が装着される構成となっている。これに応じて、携帯電話機 2 0 0 は、メモリカード 1 2 0 とデータバス B S 2 との間のデータの授受を制御するためのメモリインタフェース 1 2 0 0 をさらに備えている。

【 0 0 6 4 】

さらに、携帯電話機 2 0 0 の構成では、音楽再生モジュール 1 5 0 0 の構成も、携帯電話機 1 0 0 の構成と異なる。

【 0 0 6 5 】

すなわち、携帯電話機 2 0 0 の音楽再生モジュール 1 5 0 0 は、メモリカード 1 2 0 と携帯電話機の他の部分とのデータ授受にあたり、データバス B S 2 上においてやり取りされるデータを暗号化するための後に説明するセッションキー K s を乱数等により発生するセッションキー発生部 1 5 0 2 と、セッションキー発生部 1 5 0 2 により生成されたセッションキー K s を暗号化して、データバス B S 2 に与えるための暗号化処理部 1 5 0 4 と、データバス B S 2 によりメモリカード 1 2 0 から伝送され、公開暗号化鍵 K P p およびセッションキー K s により暗号化コンテンツキー K c をセッションキー K s について復号して出力する復号

処理部 1506 と、公開暗号化鍵 K_P に対応し、キー K_P で暗号化されたデータを復号可能な秘密復号鍵 K_P を保持する K_P 保持部 1540 と、復号処理部 1506 の出力を受けて、メモリカード 120 から伝送され公開暗号化鍵 K_P により暗号化コンテンツキー $[K_c]$ K_P を復号するための復号処理部 1530 と、サーバ 30 から配信されメモリカード 120 中に格納された暗号化コンテンツデータ $[D_c]$ K_c を、復号処理部 1530 で復号抽出されたコンテンツキー K_c に基づいて復号するための復号処理部 1520 と、復号処理部 1520 からの復号されたコンテンツデータ D_c を受けて、音楽サーバ 30 から配信された音楽データを再生するための音楽再生部 1508 と、音楽再生部 1508 の出力と音声再生部 1112 の出力とを受けて、動作モードに応じて選択的に出力、または、両者を混合して出力するための混合部 1510 と、混合部 1510 の出力を受けて、外部に出力するためのアナログ信号に変換するデジタルアナログ変換部 1512 とを含む。

【0066】

携帯電話機 200 のその他の部分は、実施の形態 1 の携帯電話機 100 の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【0067】

なお、図 4 においても、説明の簡素化のため本発明の音楽データの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

【0068】

また、図 4 に示した構成において、音楽再生部 1508、 K_P 保持部 1540、復号処理部 1530、復号処理部 1520、復号処理部 1506、暗号化処理部 1504 および K_s 発生部 1502 を、TRM に組み込む構成とすることが可能である。

【0069】

このような構成とすることで、すくなくとも、復号鍵および平文化されたデータを外部から参照できないため、携帯電話機 200 の暗号化方式および秘密復号鍵を外部から不正に取得することが困難となり、セキュリティが向上する。

【 0 0 7 0 】

さらに、図 4 において実線で囲んだ領域に相当する音楽再生モジュール 1 5 0 0 を、TRM とすることも可能である。このような構成とすれば、音楽データ等の著作権の存在するコンテンツデータの最終的なデジタルデータについても、保護することが可能である。

【 0 0 7 1 】

〔暗号／復号鍵の構成〕

図 5 は、図 4 に示した携帯電話機 2 0 0 において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

【 0 0 7 2 】

まず、図 4 に示した構成において、メモ리카ード 1 2 0 内のデータ処理を管理するための鍵としては、メモ리카ードに固有な公開暗号化鍵 $K P m$ と、公開暗号化鍵 $K P m$ により暗号化されたデータを復号するためのキー $K P m$ とは非対称な秘密復号鍵 $K m$ とがある。

【 0 0 7 3 】

ここで、キー $K P m$ とキー $K m$ とが非対称とは、複数の公開暗号化鍵 $K P m$ により暗号化されたデータが、キー $K P m$ とは異なり $K P m$ からは容易に類推できない復号鍵 $K m$ により復号できることを意味する。

【 0 0 7 4 】

したがって、メモ리카ード 1 2 0 と携帯電話機 2 0 0 とのセッションキーの授受にあたっては、後に説明するようにこれら暗号化鍵 $K m$ 、復号鍵 $K P m$ が用いられることになる。

【 0 0 7 5 】

さらに、メモ리카ード外でのデータの授受における秘密保持のための暗号化鍵としては、携帯電話機という再生装置に固有な公開暗号化鍵を $K P p$ と、音楽再生モジュール管理の鍵として、このキー $K P p$ で暗号化されたデータを復号化でき、キー $K P p$ とは非対称な秘密復号鍵 $K p$ と、各通信ごとに $K s$ 発生器 1 5 0 2 において生成される共通鍵 $K s$ とが用いられる。

【 0 0 7 6 】

ここで、共通鍵 K_s は、たとえば、携帯電話機200とメモリカード120との間のコンテンツデータの授受のためのアクセスが行なわれるごとに K_s 発生器1502において発生する。

【0077】

以下では、このような通信の単位あるいはアクセスの単位を「セッション」と呼ぶことにし、共通鍵 K_s を「セッションキー」とも呼ぶことにする。

【0078】

したがって、セッションキー K_s は各通信セッションに固有の値を有することになり、音楽再生モジュール1500において管理される。

【0079】

さらに、メモリカード120に記録される著作物データについては、まず、コンテンツデータ（音楽データ）自体を暗号化するための共通鍵であるコンテンツキー K_c があり、このコンテンツキー K_c により暗号化コンテンツデータが復号（平文化）されるものとする。

【0080】

著作権の存在するコンテンツデータ D_c は、上述のとおり、たとえば音楽データであり、このコンテンツデータをコンテンツキー K_c で復号化可能なデータを、暗号化コンテンツデータ $[D_c] K_c$ と呼ぶ。

【0081】

また、配信サーバ10から携帯電話機200に向けて、コンテンツキー K_c が配信される場合には、このコンテンツキー K_c は、すくなくとも公開暗号化鍵 K_{Pp} により暗号化されており、メモリカード120中には、この暗号化コンテンツキー $[K_c] K_p$ として格納されているものとする。

【0082】

〔メモリカードの構成〕

図6は、図4に示したメモリカード120の構成を説明するための概略ブロック図である。

【0083】

メモリカード120は、メモリインタフェース1200との間で信号を端子1

202を介して授受するデータバスBS3と、公開暗号化鍵K P mの値を保持し、データバスBS3に公開暗号化鍵K P mを出力するためのK P m保持部1401と、カード120に対応する秘密復号鍵K mを保持するためのK m保持部1402と、データバスBS3にメモリインタフェース1200から与えられるデータから、秘密復号鍵K mにより復号処理をすることにより、セッションキーK sを抽出する復号処理部1404と、データバスBS3から、公開暗号化鍵K pで暗号化されているコンテンツキーK cおよびコンテンツキーK cにより暗号化されている暗号化コンテンツデータ[D c] K cを受けて格納するためのメモリ1412と、復号処理部1404により抽出されたセッションキーK sに基づいて、メモリ1412からの出力を暗号化してデータバスBS3に与えるための暗号化処理部1406と、メモリカード120の動作を制御するためのコントローラ1420とを備える。

【0084】

なお、図6のメモリカード120内も、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールTRMに組込まれる構成とすることも可能である。

【0085】

〔再生処理〕

図7は、携帯電話機200内において、メモリカード120に保持された暗号化コンテンツデータから、音楽情報を復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

【0086】

図7を参照して、携帯電話機のキーボード1108等からのユーザの指示により、再生リクエストがメモリカード120に対して出力される（ステップS200）。

【0087】

メモリカード120においては、この再生リクエストに応じて、コントローラ1420は、K P m保持部1401から、データバスBS3、端子1202およ

びメモリインタフェース 1200 を介して、公開暗号化鍵 K_{Pm} を携帯電話機 200 に対して送信する（ステップ S202）。

【0088】

携帯電話機 200 では、カード 120 からのキー K_{Pm} を受信すると（ステップ S204）、 K_s 発生部 1502 においてセッションキー K_s を生成し（ステップ S206）、暗号化処理部 1504 が、キー K_{Pm} により、セッションキー K_s を暗号化して暗号化セッションキー $[K_s] K_{Pm}$ を生成し、データベース BS2 を介して、カード 120 に対して送信する（ステップ S208）。

【0089】

メモリカード 120 は、携帯電話機 200 により生成された暗号化セッションキー $[K_s] K_{Pm}$ を受け取り、復号処理部 1404 において秘密復号鍵 K_m により復号し、セッションキー K_s を抽出する（ステップ S210）。

【0090】

続いて、メモリカード 120 は、メモリ 1412 から、コンテンツキー $[K_c] K_p$ を読出す（ステップ S212）。

【0091】

続いて、メモリカード 120 は、暗号化処理部 1406 において抽出したセッションキー K_s により、暗号化コンテンツキー $[K_c] K_p$ を暗号化し、暗号化された暗号化コンテンツキー $[[K_c] K_p] K_s$ をデータベース BS2 に与える（ステップ S214）。

【0092】

携帯電話機 200 の復号処理部 1506 は、メモリカード 120 から送信された暗号化された暗号化コンテンツキー $[[K_c] K_p] K_s$ をセッションキー K_s により復号処理を行なうことにより、暗号化コンテンツキー $[K_c] K_p$ を取得する（ステップ S216）。

【0093】

さらに、携帯電話機 200 の復号処理部 1530 は、 K_p 保持部 1540 からのキー K_p に基づいて、データ $[K_c] K_p$ の復号処理を行なう（ステップ S218）。

【0094】

復号処理部1530が復号処理により、コンテンツキーKcを抽出できた場合は（ステップS220）、処理は次のステップS222に進み、抽出できない場合は（ステップS220）、処理は終了する（ステップS226）。

【0095】

復号処理部1530が復号処理により、コンテンツキーKcを抽出できた場合は、メモリカード120は、暗号化コンテンツデータ[Dc] Kcをメモリ1412から読出し、データバスBS2に与える（ステップS222）。

【0096】

携帯電話機200の復号処理部1520は、暗号化コンテンツデータ[Dc] Kcを、抽出されたコンテンツキーKcにより復号処理して平文のコンテンツデータDcを生成し、音楽再生部1508は、コンテンツデータDcを再生して混合部1510に与える。デジタルアナログ変換部1512は、混合部1510からのデータを受け取ってアナログ信号に変換し、外部に再生された音楽を出力し、処理が終了する（ステップS226）。

【0097】

このような構成とすることで、携帯電話機200において生成されたセッションキーに基づいてコンテンツキーを暗号化した上で、メモリカード120から携帯電話機200に送信して再生動作を行なうことが可能となる。

【0098】

以上のような構成により、実施の形態1の携帯電話機100の奏する効果に加えて、実施の形態2の携帯電話機200においては、携帯電話機200に対して、着脱可能なメモリカード内に配信データが格納される構成となっているので、配信を受けたり、再生する際にのみメモリカードを装着すれば足りるため、重量等の観点から携帯機としての利便性が損なわれることがない。

【0099】

しかも、携帯電話機とメモリカードとの間のデータの授受は、セッションキーにより暗号化された上で行なわれるので、データに対するセキュリティが向上し、著作権者およびユーザの双方の権利を保護することが可能となる。

【0100】

さらに、配信を受けた後は、メモリカードをほかの再生装置に装着することで、再生を行なうことも可能となり、ユーザの音楽データ利用の自由度が向上する。

【0101】

〔実施の形態3〕

図8は、本発明の実施の形態3の携帯電話機300の構成を説明するための概略ブロック図であり、実施の形態2の図4と対比される図である。

【0102】

図8に示した実施の形態3の携帯電話機300の構成と、実施の形態2の携帯電話機200の構成が異なる点は、以下のとおりである。

【0103】

まず、図8においては、携帯電話機300には、携帯電話機300により受信された暗号化された音楽データを受取って格納し、暗号化コンテンツデータおよび暗号化コンテンツキーをさらに所定の暗号化処理をした上で、携帯電話機300中の音楽再生モジュール1500に与えるための着脱可能なメモリカード130が装着される構成となっている。

【0104】

メモリカード130は、後に説明するように、メモリカード130自身でセッションキーKs2を生成する点で、メモリカード120と異なる。

【0105】

さらに、携帯電話機300の構成では、音楽再生モジュール1500の構成も、携帯電話機200の構成と異なる。

【0106】

すなわち、携帯電話機300の音楽再生モジュール1500は、メモリカード130と携帯電話機の他の部分とのデータ授受にあたり、データバスBS2上においてやり取りされるデータを暗号化するためのセッションキーKs1を乱数等により発生するセッションキー発生部1552と、セッションキー発生部1552により生成されたセッションキーKs1をメモリカード130からのセッショ

ンキー K s 2 で暗号化して、データバス B S 2 に与えるための暗号化処理部 1 5 5 4 と、データバス B S 2 によりメモリカード 1 3 0 から伝送され、公開暗号化鍵 K P p およびセッションキー K s 1 により暗号化コンテンツキー K c をセッションキー K s 1 について復号して出力する復号処理部 1 5 5 6 と、コントローラ 1 1 0 6 により制御されて、データバス B S 2 により伝達された暗号化されたメモリカード 1 3 0 のセッションキー [K s 2] K p または復号処理部 1 5 5 6 から出力された暗号化コンテンツキー [K c] K p のいずれかを、公開暗号化鍵 K P p により暗号化されたデータを復号するための復号処理部 1 5 3 0 に与える切換え回路 1 5 5 0 とを含む。

【0107】

暗号化処理部 1 5 5 4 は、復号処理部 1 5 3 0 において秘密復号鍵 K p により復号されて抽出されたメモリカード 1 3 0 のセッションキー K s 2 を受けて、セッションキー発生部 1 5 5 2 により生成されたセッションキー K s 1 をセッションキー K s 2 で暗号化処理する。

【0108】

携帯電話機 3 0 0 のその他の部分は、実施の形態 2 の携帯電話機 2 0 0 の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【0109】

なお、図 8 においても、説明の簡素化のため本発明の音楽データの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

【0110】

また、図 8 に示した構成において、音楽再生部 1 5 0 8、K p 保持部 1 5 4 0、復号処理部 1 5 3 0、復号処理部 1 5 2 0、復号処理部 1 5 5 6、暗号化処理部 1 5 5 4、セッションキー発生部 1 5 5 2 および切換え回路 1 5 5 0 を、T R M に組み込む構成とすることが可能である。

【0111】

このような構成とすることで、すくなくとも、復号鍵および平文化されたデータを外部から参照できないため、携帯電話機 3 0 0 の暗号化方式および秘密復号

鍵を外部から不正に取得することが困難となり、セキュリティが向上する。

【0112】

さらに、図8において実線で囲んだ領域に相当する音楽再生モジュール1500を、TRMとすることも可能である。このような構成とすれば、音楽データ等の著作権の存在するコンテンツデータの最終的なデジタルデータについても、保護することが可能である。

【0113】

[暗号／復号鍵の構成]

図9は、図8に示した携帯電話機300において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

【0114】

まず、図8に示した構成において、メモ리카ード130内のデータ処理を管理するための鍵としては、メモ리카ードに固有な公開暗号化鍵 K_{Pm} と、公開暗号化鍵 K_{Pm} により暗号化されたデータを復号するためのキー K_{Pm} とは非対称な秘密復号鍵 K_m と、メモ리카ード130が生成し各セッションに固有なセッションキー K_{s2} とがある。

【0115】

したがって、メモ리카ード130と携帯電話機300とのセッションキーの授受にあたっては、後に説明するようにこれら暗号鍵 K_m 、復号鍵 K_{Pm} 、セッションキー K_{s2} が用いられることになる。

【0116】

さらに、メモ리카ード外でのデータの授受における秘密保持のための暗号鍵としては、携帯電話機という再生装置に固有な公開暗号化鍵であって、コンテンツデータの配信時にコンテンツデータとともに配信され、後に説明するようにメモ리카ード130内に記憶される公開暗号鍵 K_{Pp} と、音楽再生モジュールの管理の鍵として、このキー K_{Pp} で暗号化されたデータを復号化でき、キー K_{Pp} とは非対称な秘密復号鍵 K_p と、各アクセスごとにセッションキー発生器1552において生成される共通鍵であるセッションキー K_{s1} とが用いられる。

【0117】

セッションキー K_{s1} も各通信セッションに固有の値を有することになり、音楽再生モジュール 1 5 0 0 において管理される。

【0 1 1 8】

さらに、メモ리카ード 1 3 0 に記録される著作物データについては、まず、音楽データ（コンテンツデータ）自体を暗号化するための共通鍵であるコンテンツキー K_c があり、このコンテンツキー K_c により暗号化コンテンツデータが復号（平文化）されるものとする。

【0 1 1 9】

また、配信サーバ 1 0 から携帯電話機 3 0 0 に向けて、コンテンツキー K_c が配信される場合には、このコンテンツキー K_c は、すくなくとも公開暗号化鍵 K_{Pp} により暗号化されており、メモ리카ード 1 3 0 中には、この暗号化コンテンツキー $[K_c]_{K_{Pp}}$ として格納されているものとする。

【0 1 2 0】

さらに、著作権の存在するコンテンツデータ D_c は、このコンテンツデータをコンテンツキー K_c で復号化可能な暗号化コンテンツデータ $[D_c]_{K_c}$ としてメモ리카ード 1 3 0 に格納されているものとする。

【0 1 2 1】

〔メモ리카ードの構成〕

図 1 0 は、図 8 に示したメモ리카ード 1 3 0 の構成を説明するための概略ブロック図である。

【0 1 2 2】

メモ리카ード 1 3 0 は、メモリアインタフェース 1 2 0 0 との間で信号を端子 1 2 0 2 を介して授受するデータバス B_{S3} と、セッション毎にセッションキー K_{s2} を生成するためのセッションキー発生部 1 4 5 0 と、セッションキー K_{s2} を公開暗号化鍵 K_{Pp} で暗号化してデータバス B_{S3} に与えるための暗号化処理部 1 4 5 2 と、データバス B_{S3} にメモリアインタフェース 1 2 0 0 から与えられるデータ $[K_{s1}]_{K_{s2}}$ から、セッションキー K_{s2} により復号処理をすることにより、携帯電話機 3 0 0 からのセッションキー K_{s1} を抽出する復号処理部 1 4 5 4 と、データバス B_{S3} から、公開暗号化鍵 K_{Pp} と、公開暗号化鍵 K_P

pで暗号化されているコンテンツキー [Kc] KpとコンテンツキーKcにより暗号化されている暗号化コンテンツデータ [Dc] Kcとの3つを受けて格納するためのメモリ1412と、復号処理部1454により抽出されたセッションキーKs1に基づいて、メモリ1412からの出力を暗号化してデータバスBS3に与えるための暗号化処理部1456と、メモリカード130の動作を制御するためのコントローラ1420とを備える。

【0123】

なお、図10のメモリカード130内も、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールTRMに組込まれる構成とすることも可能である。

【0124】

〔再生処理〕

図11は、携帯電話機300内において、メモリカード130に保持された暗号化コンテンツデータから、音楽情報を復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

【0125】

図11を参照して、携帯電話機のキーボード1108等からのユーザの指示により、再生リクエストがメモリカード130に対して出力される（ステップS300）。

【0126】

メモリカード130においては、この再生リクエストに応じて、コントローラ1420は、セッションキー発生部1450を制御してセッションキーKs2を発生させる（ステップS302）。コントローラ1420の制御により、このセッションキーKs2を暗号化処理部1452は公開暗号化鍵Kppにより暗号化して暗号化セッションキー [Ks2] Kpを生成し、この暗号化セッションキー [Ks2] Kpを、データバスBS3、端子1202およびメモリインタフェース1200を介して、携帯電話機300に対して送信する（ステップS304）。

【0127】

携帯電話機300では、カード130からの暗号化セッションキー [Ks2] Kpを受信すると、切換え回路1550を介して復号処理部1530が暗号化セッションキー [Ks2] Kpを受けて復号しセッションキーKs2を獲得する（ステップS306）。

【0128】

携帯電話機300においては、セッションキー発生部1552においてセッションキーKs1を生成し（ステップS308）、暗号化処理部1554が、ステップS306において抽出されたセッションキーKs2により、セッションキーKs1を暗号化して暗号化セッションキー [Ks1] Ks2を生成し、データバスBS2を介して、カード130に対して送信する（ステップS310）。

【0129】

メモリカード130は、携帯電話機300により生成され、かつ暗号化されたセッションキー [Ks1] Ks2を受け取り、復号処理部1454においてセッションキーKs2により復号し、セッションキーKs1を抽出する（ステップS312）。

【0130】

続いて、メモリカード130は、メモリ1412から、暗号化コンテンツキー [Kc] Kpを読み出し（ステップS314）、暗号化処理部1456において、抽出したセッションキーKs1により、暗号化コンテンツキー [Kc] Kpを暗号化し、暗号化された暗号化コンテンツキー [[Kc] Kp] Ks1をデータバスBS3等を介してデータバスBS2に与える（ステップS316）。

【0131】

携帯電話機300の復号処理部1556は、メモリカード130から送信された暗号化された暗号化コンテンツキー [[Kc] Kp] Ks1に対してセッションキーKs1により復号処理を行なうことにより、暗号化コンテンツキー [Kc] Kpを取得する（ステップS318）。

【0132】

さらに、携帯電話機300の復号処理部1530は、切換え回路1550を介

して暗号化コンテンツキー [Kc] Kpを受け、Kp保持部1540からのキーKpに基づいて、暗号化コンテンツキー [Kc] Kpの復号処理を行なう（ステップS320）。

【0133】

復号処理部1530が復号処理により、コンテンツキーKcを抽出できた場合は（ステップS322）、処理は次のステップS324に進み、抽出できない場合は（ステップS322）、処理は終了する（ステップS330）。

【0134】

復号処理部1530が復号処理により、コンテンツキーKcを抽出できた場合は、メモリカード130は、暗号化コンテンツデータ [Dc] Kcをメモリ1412から読出し、データバスBS3等を介してデータバスBS2に与える（ステップS324）。

【0135】

携帯電話機300の復号処理部1520は、暗号化コンテンツデータ [Dc] Kcを、抽出されたコンテンツキーKcにより復号処理して平文のコンテンツデータDcを生成し、音楽再生部1508は、コンテンツデータDcを再生して混合部1510に与える。デジタルアナログ変換部1512は、混合部1510からのデータを受け取ってアナログ信号に変換し、外部に再生された音楽を出力し（ステップS328）、処理が終了する（ステップS330）。

【0136】

このような構成とすることで、携帯電話機300において生成されたセッションキーKs1に基づいて暗号化コンテンツキー [Kc] Kpを暗号化した上で、メモリカード130から携帯電話機300に送信して再生動作を行なうことが可能となる。しかも、メモリカード130においてセッション毎に生成されたセッションキーKs2により暗号化した上で、メモリカード130と携帯電話機300との間でセッションキーKs1の授受が行なわれるので、実施の形態2よりも一層、セキュリティが向上し、著作権者およびユーザの双方の権利を保護することが可能となる。

【0137】

また、以上のような構成により、実施の形態 3 の携帯電話機 300 においても、携帯電話機 300 に対して、着脱可能なメモリカード内に配信データが格納される構成となっているので、配信を受けたり、再生する際にのみメモリカードを装着すれば足りるため、重量等の観点から携帯機としての利便性が損なわれることがない。

【0138】

さらに、配信を受けた後は、メモリカードをほかの再生装置に装着することで、再生を行なうことも可能となり、ユーザの音楽データ利用の自由度が向上する。

【0139】

〔実施の形態 4〕

図 12 は、本発明の実施の形態 4 の携帯電話機 400 の構成を説明するための概略ブロック図であり、実施の形態 3 の図 8 と対比される図である。

【0140】

図 12 に示した実施の形態 4 の携帯電話機 400 の構成と、実施の形態 3 の携帯電話機 300 の構成が異なる点は、以下のとおりである。

【0141】

すなわち、図 12 においては、携帯電話機 400 には、携帯電話機 400 により受信された暗号化コンテンツデータおよび暗号化コンテンツキーを受取って格納し、さらに所定の暗号化処理をした上で、携帯電話機 400 中の音楽再生モジュール 1500 に与えるための着脱可能なメモリカード 140 が装着される構成となっている。メモリカード 140 は、後に説明するように、携帯電話機 400 に対する認証機能を有する点で実施の形態 3 のメモリカード 130 と異なる。

【0142】

さらに、携帯電話機 400 の構成では、音楽再生モジュール 1500 の構成も、携帯電話機 300 の構成と異なる。

【0143】

すなわち、携帯電話機 400 の音楽再生モジュール 1500 は、メモリカード 140 と携帯電話の他の部分とのデータ授受にあたり、携帯電話機 400 に対す

る認証機能を実現するために、再生装置である携帯電話機400のクラス（種類等）に固有な公開暗号鍵K P pと認証データC r t fとを、システムに共通な公開復号鍵（公開認証鍵）K P m aにより暗号化して保持する〔K P p、C r t f〕K P m a保持部1560をさらに備える構成となっている点である。

【0144】

携帯電話機400のその他の部分は、実施の形態3の携帯電話機300の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【0145】

なお、図12においても、説明の簡素化のため本発明の音楽データの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

【0146】

また、図12に示した構成において、音楽再生部1508、K p保持部1540、復号処理部1530、復号処理部1520、復号処理部1556、暗号化処理部1554、セッションキー発生部1552、切換え回路1550および〔K P p、C r t f〕K P m a保持部1560を、TRMに組み込む構成とすることが可能である。

【0147】

このような構成とすることで、すくなくとも、認証データ、復号鍵および平文化されたデータを外部から変更あるいは参照できないため、携帯電話機400の暗号化方式および秘密復号鍵を外部から不正に取得することが困難となり、セキュリティが向上する。

【0148】

さらに、図12において実線で囲んだ領域に相当する音楽再生モジュール1500を、TRMとすることも可能である。このような構成とすれば、音楽データ等の著作権の存在するデータの最終的なデジタルデータについても、保護することが可能である。

【0149】

〔暗号／復号鍵の構成〕

図 1 3 は、図 1 2 に示した携帯電話機 4 0 0 において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

【0 1 5 0】

まず、図 1 2 に示した構成において、メモ리카ード 1 4 0 内のデータ処理を管理するための鍵としては、システムに共通な公開復号鍵であり、認証鍵の機能を有する $K P m a$ と、メモ리카ード 1 4 0 が生成し各セッションに固有な共通鍵であるセッションキー $K s 2$ とがある。

【0 1 5 1】

さらに、メモ리카ード外でのデータの授受における秘密保持のための暗号鍵としては、音楽再生モジュールの管理の鍵として、携帯電話機という再生装置のクラスに固有な公開暗号化鍵であって、上述のとおり、鍵 $K P m a$ により暗号化された形で携帯電話機 4 0 0 中の $[K P p, C r t f]$ $K P m a$ 保持部 1 5 6 0 に格納されている公開暗号鍵 $K P p$ と、このキー $K P p$ で暗号化されたデータを復号化でき、キー $K P p$ とは非対称な秘密復号鍵 $K p$ と、各アクセスごとにセッションキー発生器 1 5 5 2 において生成される共通鍵であるセッションキー $K s 1$ とが用いられる。

【0 1 5 2】

セッションキー $K s 1$ も各通信セッションに固有の値を有することになり、音楽再生モジュール 1 5 0 0 において管理される。

【0 1 5 3】

なお、「再生装置のクラス」とは、再生装置ごと、あるいは、再生装置の種類（製造メーカ、製造ロット）ごとに、この再生装置を区別するための区分であるものとする。

【0 1 5 4】

さらに、メモ리카ード 1 4 0 に記録される著作物データについては、まず、コンテンツデータ（音楽データ）自体を暗号化するための共通鍵であるコンテンツキー $K c$ があり、このコンテンツキー $K c$ により暗号化コンテンツデータが復号（平文化）されるものとする。

【0 1 5 5】

また、配信サーバ10から携帯電話機400に向けて、コンテンツキーKcが配信される場合には、このコンテンツキーKcは、すくなくとも公開暗号化鍵Kpにより暗号化されており、メモリカード140中には、この暗号化コンテンツキー[Kc]Kpとして格納されているものとする。

【0156】

さらに、著作権の存在するコンテンツデータDcは、このコンテンツデータをコンテンツキーKcで復号化可能な暗号化コンテンツデータ[Dc]Kcとしてメモリカード140に格納されているものとする。

【0157】

[メモリカードの構成]

図14は、図12に示したメモリカード140の構成を説明するための概略ブロック図である。

【0158】

メモリカード140の構成が、実施の形態3のメモリカード130の構成と異なる点は、まず、コントローラ1420に制御されて、データバスBS3上のデータに対して公開復号鍵Kpmaによる復号処理を行い、携帯電話機140からの公開暗号鍵Kppおよび認証データCrtfの取得を行うための復号処理部1460を備える構成となっている点である。したがって、暗号化処理部1452は、復号処理部1460からの公開暗号化鍵Kppに基づいて暗号化処理を行う。

【0159】

さらに、メモリカード140中のメモリ1412においては、メモリカード130の場合に保持されていた公開暗号化鍵Kppの代わりに、公開復号鍵Kpmaが格納されている。したがって、復号処理部1460は、メモリ1412中に保持された公開復号鍵Kpmaに基づいて復号処理を行う。

【0160】

メモリカード140のその他の部分は、実施の形態3のメモリカード130の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【0161】

なお、図14のメモリカード140内も、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内の鍵等の読出を不能化するためのモジュールTRMに組込まれる構成とすることも可能である。

【0162】

〔再生処理〕

図15は、携帯電話機400内において、メモリカード140に保持された暗号化コンテンツデータから、音楽を再生して外部に出力するための再生処理を説明するフローチャートである。

【0163】

図15を参照して、再生処理の説明を行なう。携帯電話機のキーボード1108等からのユーザの指示により、再生リクエストが与えられると（ステップS400）、携帯電話機400の〔K P p, C r t f〕K P m a保持部1560からメモリカード140に対してデータ〔K P p, C r t f〕K P m aが出力される（ステップS402）。

【0164】

メモリカード140においては、このデータ〔K P p, C r t f〕K P m aを復号部1460により復号し、公開暗号化鍵K P pと認証データC r t fとを獲得する（ステップS406）。コントローラ1420は、認証データC r t fに基づいて携帯電話機400の認証を行ない（ステップS406）、携帯電話機400が正規の機器であれば処理をステップS408に移行し、携帯電話機400が正規の機器でない場合、再生のための動作を行わずに処理を終了する（ステップS434）。

【0165】

携帯電話機400が正規の機器である場合、コントローラ1420は、セッションキー発生部1450を制御してセッションキーK s 2を発生させる（ステップS408）。コントローラ1420の制御により、このセッションキーK s 2を暗号化処理部1452は公開暗号化鍵K P pにより暗号化して暗号化セッショ

ンキー [K s 2] K p を生成し、この暗号化セッションキー [K s 2] K p を、データバス B S 3、端子 1 2 0 2 およびメモリインタフェース 1 2 0 0 を介して、携帯電話機 4 0 0 に対して送信する（ステップ S 4 1 0）。

【0166】

携帯電話機 4 0 0 では、カード 1 4 0 からの暗号化セッションキー [K s 2] K p を受信すると、切換え回路 1 5 5 0 を介して復号処理部 1 5 3 0 が暗号化セッションキー [K s 2] K p を受けて復号しセッションキー K s 2 を獲得する（ステップ S 4 1 2）。

【0167】

携帯電話機 4 0 0 においては、セッションキー発生部 1 5 5 2 においてセッションキー K s 1 を生成し（ステップ S 4 1 4）、暗号化処理部 1 5 5 4 が、ステップ S 4 1 2 において抽出されたセッションキー K s 2 により、セッションキー K s 1 を暗号化してデータ [K s 1] K s 2 を生成し、データバス B S 2 を介して、カード 1 4 0 に対して送信する（ステップ S 4 1 6）。

【0168】

メモリカード 1 4 0 は、携帯電話機 4 0 0 により生成され、かつ暗号化されたセッションキー [K s 1] K s 2 を受け取り、復号処理部 1 4 5 4 においてセッションキー K s 2 により復号し、セッションキー K s 1 を抽出する（ステップ S 4 1 8）。

【0169】

続いて、メモリカード 1 4 0 は、メモリ 1 4 1 2 から、暗号化されているデータ [K c] K p を読出し（ステップ S 4 2 0）、暗号化処理部 1 4 5 6 において、抽出したセッションキー K s 1 により、暗号化コンテンツキー [K c] K p を暗号化し、暗号化された暗号化コンテンツキー [[K c] K p] K s 1 をデータバス B S 3 等を介してデータバス B S 2 に与える（ステップ S 4 2 2）。

【0170】

携帯電話機 4 0 0 の復号処理部 1 5 5 6 は、メモリカード 1 4 0 から送信された暗号化された暗号化コンテンツキー [[K c] K p] K s 1 に対してセッションキー K s 1 により復号処理を行なうことにより、暗号化コンテンツキー [K c

] K_pを取得する(ステップS424)。

【0171】

さらに、携帯電話機400の復号処理部1530は、切換え回路1550を介して暗号化コンテンツキー[K_c] K_pを受け、K_p保持部1540からのキーK_pに基づいて、データ[K_c] K_pの復号処理を行なう(ステップS426)。

【0172】

復号処理部1530が、復号処理によりコンテンツキーK_cを抽出できた場合は(ステップS428)、処理は次のステップS430に進み、抽出できない場合は(ステップS428)、処理は終了する(ステップS434)。

【0173】

復号処理部1530が復号処理により、コンテンツキーK_cを抽出できた場合は、メモリカード140は、暗号化コンテンツデータ[D_c] K_cをメモリ1412から読出し、データバスBS3等を介してデータバスBS2に与える(ステップS430)。

【0174】

携帯電話機400の復号処理部1520は、暗号化コンテンツデータ[D_c] K_cを、抽出されたコンテンツキーK_cにより復号処理して平文の音楽データD_cを生成し、音楽再生部1508は、コンテンツデータD_cを再生して混合部1510に与える。デジタルアナログ変換部1512は、混合部1510からのデータを受け取って変換し、外部に再生された音楽を出力し(ステップS432)、処理が終了する(ステップS434)。

【0175】

このような構成とすることで、実施の形態3の携帯電話機300およびメモリカード130の奏する効果に加えて、携帯電話機400からのデータ[K_p, C_rt_f] K_p_{ma}に基づいて、メモリカード140が認証の結果、正規の機器と判断された携帯電話機400とメモリカード140の間でしか再生動作が行なわれないため、システムのセキュリティの向上と、著作権者の著作権の保護を図ることが可能となる。

【0 1 7 6】

〔実施の形態 5〕

図 1 6 は、本発明の実施の形態 5 の携帯電話機 5 0 0 の構成を説明するための概略ブロック図であり、実施の形態 4 の図 1 2 と対比される図である。

【0 1 7 7】

図 1 6 に示した実施の形態 5 の携帯電話機 5 0 0 の構成と、実施の形態 4 の携帯電話機 4 0 0 の構成が異なる点は、以下のとおりである。

【0 1 7 8】

すなわち、図 1 6 においては、メモ리카ード 1 4 0 に代わりメモ리카ード 1 5 0 が装着されており、さらに、メモ리카ード 1 5 0 から携帯電話機 5 0 0 に対してコンテンツキー K c を送信する場合は、セッションキー K s 1 により暗号化されたデータ [K c] K s 1 として送信される。したがって、実施の形態 4 の場合のように、コンテンツキー K c の送信の際に、キー K P p とキー K s 1 により 2 重に暗号化されているわけではないため、キー K s 1 による復号処理とキー K p による復号処理とは、独立に行なうことが可能となり、図 1 6 に示した携帯電話機 5 0 0 においてはにおいては切換スイッチ 1 5 5 0 が省略されている。

【0 1 7 9】

すなわち、携帯電話機 5 0 0 の音楽再生モジュール 1 5 0 0 は、秘密復号鍵 K p を保持するための K p 保持部 1 5 4 0 と、メモ리카ード 1 5 0 からデータバス B s 2 を介して与えられるデータ [K s 2] K p をキー K p により復号化するための復号処理部 1 5 3 0 と、メモ리카ード 1 5 0 と携帯電話機の他の部分とのデータ授受にあたり、データバス B S 2 上においてやり取りされるデータを暗号化するためのセッションキー K s 1 を乱数等により発生するセッションキー発生部 1 5 5 2 と、セッションキー発生部 1 5 5 2 により生成されたセッションキー K s 1 をメモ리카ード 1 5 0 からのセッションキー K s 2 で暗号化して、データバス B S 2 に与えるための暗号化処理部 1 5 5 4 と、データバス B S 2 によりメモ리카ード 1 5 0 から伝送され、セッションキー K s 1 により暗号化コンテンツキー K c をセッションキー K s 1 について復号して出力する復号処理部 1 5 5 6 と、復号処理部 1 5 5 6 から出力されるコンテンツキー K c に基づいて、データバ

スBs2を介してメモリカード150から与えられる暗号化コンテンツデータ[Dc]Kcを復号して音楽再生部1508に与えるための復号処理部1520と、メモリカード150と携帯電話の他の部分とのデータ授受にあたり、携帯電話機500に対する認証機能を実現するために、再生装置である携帯電話機500のクラス(種類等)に固有な公開暗号鍵Kppと認証データCr tfとを、システムに共通な公開復号鍵Kpmaにより暗号化して保持する[Kpp、Cr tf]Kpma保持部1560とを備える。

【0180】

携帯電話機500のその他の部分は、実施の形態4の携帯電話機400の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【0181】

なお、図16においても、説明の簡素化のため本発明のコンテンツデータの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

【0182】

また、図16に示した構成においても、音楽再生部1508、Kp保持部1540、復号処理部1530、復号処理部1520、復号処理部1556、暗号化処理部1554、セッションキー発生部1552および[Kpp、Cr tf]Kpma保持部1560を、TRMに組み込む構成とすることが可能である。

【0183】

このような構成とすることで、すくなくとも、認証データ、復号鍵および平文化されたデータを外部から変更あるいは参照できないため、携帯電話機500の暗号化方式および秘密復号鍵を外部から不正に取得することが困難となり、セキュリティが向上する。

【0184】

さらに、図16において実線で囲んだ領域に相当する音楽再生モジュール1500を、TRMとすることも可能である。このような構成とすれば、音楽データ等の著作権の存在するコンテンツデータの最終的なデジタルデータについても、保護することが可能である。

【0 1 8 5】

[メモ리카ードの構成]

図 1 7 は、図 1 6 に示したメモ리카ード 1 5 0 の構成を説明するための概略ブロック図である。

【0 1 8 6】

メモ리카ード 1 5 0 の構成が、実施の形態 4 のメモ리카ード 1 4 0 の構成と異なる点は、コンテンツキー K c がメモリ 1 4 1 2 中に暗号化されることなく、平分データとして格納されている点である。

【0 1 8 7】

メモ리카ード 1 5 0 のその他の部分は、実施の形態 4 のメモ리카ード 1 4 0 の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【0 1 8 8】

なお、図 1 7 のメモ리카ード 1 5 0 内も、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュール T R M に組込まれる構成とする。

【0 1 8 9】

[再生処理]

図 1 8 は、携帯電話機 5 0 0 内において、メモ리카ード 1 5 0 に保持された暗号化コンテンツデータから、音楽情報を復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

【0 1 9 0】

図 1 8 を参照して、再生処理についての説明を行なう。携帯電話機のキーボード 1 1 0 8 等からのユーザの指示により、再生リクエストが与えられると（ステップ S 5 0 0）、携帯電話機 5 0 0 の [K P p, C r t f] K P m a 保持部 1 5 6 0 からメモ리카ード 1 5 0 に対してデータ [K P p, C r t f] K P m a が出力される（ステップ S 5 0 2）。

【0 1 9 1】

メモリカード150においては、このデータ[KPp, Crtf] KPmaを復号部1460により復号し、公開暗号化鍵KPpと認証データCrtfとを獲得する(ステップS506)。コントローラ1420は、認証データCrtfに基づいて携帯電話機500の認証を行ない(ステップS506)、携帯電話機500が正規の機器であれば処理をステップS508に移行し、携帯電話機500が正規の機器でない場合、再生のための動作を行わずに処理を終了する(ステップS534)。

【0192】

携帯電話機500が正規の機器である場合、コントローラ1420は、セッションキー発生部1450を制御してセッションキーKs2を発生させる(ステップS508)。コントローラ1420の制御により、このセッションキーKs2を暗号化処理部1452は公開暗号化鍵KPpにより暗号化して暗号化セッションキー[Ks2] Kpを生成し、この暗号化セッションキー[Ks2] Kpを、データバスBS3、端子1202およびメモリインタフェース1200を介して、携帯電話機500に対して送信する(ステップS510)。

【0193】

携帯電話機500では、カード150からの暗号化セッションキー[Ks2] Kpを受信すると、切換え回路1550を介して復号処理部1530が暗号化セッションキー[Ks2] Kpを受けて復号しセッションキーKs2を獲得する(ステップS512)。

【0194】

携帯電話機500においては、セッションキー発生部1552においてセッションキーKs1を生成し(ステップS514)、暗号化処理部1554が、ステップS512において抽出されたセッションキーKs2により、セッションキーKs1を暗号化してデータ[Ks1] Ks2を生成し、データバスBS2を介して、カード150に対して送信する(ステップS516)。

【0195】

メモリカード150は、携帯電話機500により生成され、かつ暗号化されたセッションキー[Ks1] Ks2を受け取り、復号処理部1454においてセッ

セッションキー K s 2 により復号し、セッションキー K s 1 を抽出する（ステップ S 5 1 8）。

【0196】

続いて、メモリカード 1 5 0 は、メモリ 1 4 1 2 から、コンテンツキー K c を読出す（ステップ S 5 2 0）。

【0197】

続いて、メモリカード 1 5 0 は、暗号化処理部 1 4 5 6 において、抽出したセッションキー K s 1 により、コンテンツキー K c を暗号化し、暗号化コンテンツキー [K c] K s 1 をデータバス B S 3 等を介してデータバス B S 2 に与える（ステップ S 5 2 2）。

【0198】

携帯電話機 5 0 0 の復号処理部 1 5 5 6 は、メモリカード 1 5 0 から送信された暗号化された暗号化コンテンツキー [K c] K s 1 に対して、セッションキー K s 1 により復号処理を行なうことにより、コンテンツキー K c を取得する（ステップ S 5 2 4）。

【0199】

メモリカード 1 5 0 は、暗号化コンテンツデータ [D c] K c をメモリ 1 4 1 2 から読出し、データバス B S 3 等を介してデータバス B S 2 に与える（ステップ S 5 3 0）。

【0200】

携帯電話機 5 0 0 の復号処理部 1 5 2 0 は、暗号化コンテンツデータ [D c] K c を、抽出されたコンテンツキー K c により復号処理して平文のコンテンツデータ D c を生成し、音楽再生部 1 5 0 8 は、コンテンツデータ D c を再生して混合部 1 5 1 0 に与える。デジタルアナログ変換部 1 5 1 2 は、混合部 1 5 1 0 からのデータを受け取ってアナログ信号に変換し、外部に再生された音楽を出力し（ステップ S 5 3 2）、処理が終了する（ステップ S 5 3 4）。

【0201】

このような構成とすることで、実施の形態 4 の携帯電話機 4 0 0 およびメモリカード 1 3 0 の奏する効果と同様に、携帯電話機 5 0 0 からのデータ [K P p,

C r t f] K P m aに基づいて、メモリカード150が認証の結果、正規の機器と判断された携帯電話機500とメモリカード150の間でしか再生動作が行なわれないため、著作権者の著作権の保護を図ることが、より簡易な構成で可能となる。

【0202】

【実施の形態6】

図19は、本発明の実施の形態6の携帯電話機600の構成を説明するための概略ブロック図であり、実施の形態5の図16と対比される図である。

【0203】

図19に示した実施の形態6の携帯電話機600の構成と、実施の形態5の携帯電話機500の構成が異なる点は、以下のとおりである。

【0204】

すなわち、図19においては、携帯電話機600は、システム共通の秘密復号鍵K c o mを保持するためのK c o m保持部1570と、復号処理部1556の出力を受けて、秘密復号鍵K c o mにより復号してコンテンツキーK cを獲得し、復号処理部1520に与える復号処理部1572をさらに備える構成となっている。

【0205】

すなわち、実施の形態5においては、メモリカード150から携帯電話機500に対してコンテンツキーK cを送信する場合は、セッションキーK s 1により暗号化されたコンテンツキー[K c] K s 1として送信されたのに対し、実施の形態6においては、メモリカード160から携帯電話機600に対してコンテンツキーK cを送信する場合は、秘密復号鍵K c o mおよびセッションキーK s 1により復号可能なように暗号化されたコンテンツキー[[K c] K c o m] K s 1として送信される。

【0206】

携帯電話機600のその他の部分は、実施の形態5の携帯電話機500の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【0207】

なお、図 1 9 においても、説明の簡素化のため本発明の音楽データの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

【0208】

また、図 1 9 に示した構成において、音楽再生部 1 5 0 8、K p 保持部 1 5 4 0、復号処理部 1 5 3 0、復号処理部 1 5 2 0、復号処理部 1 5 5 6、暗号化処理部 1 5 5 4、セッションキー発生部 1 5 5 2、[K P p、C r t f] K P m a 保持部 1 5 6 0、K c o m 保持部および復号処理部 1 5 7 2 を、T R M に組み込む構成とすることが可能である。

【0209】

このような構成とすることで、すくなくとも、認証データ、復号鍵および平文化されたコンテンツデータを外部から不正に取得することができなくなり、セキュリティが向上する。

【0210】

さらに、図 1 9 において実線で囲んだ領域に相当する音楽再生モジュール 1 5 0 0 を、T R M とすることも可能である。このような構成とすれば、音楽データ等の著作権の存在するデータの最終的なデジタルデータについても、保護することが可能である。

【0211】

[暗号／復号鍵の構成]

図 2 0 は、図 1 9 に示した携帯電話機 6 0 0 において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

【0212】

まず、図 1 9 に示した構成において、メモリカード 1 6 0 内のデータ処理を管理するための鍵としては、システムに共通な公開復号鍵 K P m a と、メモリカード 1 6 0 が生成し各セッションに固有なセッションキー K s 2 とがある。

【0213】

さらに、メモリカード外でのデータの授受における秘密保持のための暗号鍵としては、音楽再生モジュールの管理の鍵として、携帯電話機という再生装置のク

ラスに固有な公開暗号化鍵であって、鍵 K_{Pma} により暗号化された形で携帯電話機 600 中の $[K_{Pp}, Crtf]$ K_{Pma} 保持部 1560 に格納されている公開暗号鍵 K_{Pp} と、このキー K_{Pp} で暗号化されたデータを復号化でき、キー K_{Pp} とは非対称な秘密復号鍵 K_p と、システムに共通な秘密復号鍵 K_{com} と、各アクセスごとにセッションキー発生器 1552 において生成される共通鍵であるセッションキー K_{s1} とが用いられる。

【0214】

セッションキー K_{s1} も各通信セッションに固有の値を有することになり、音楽再生モジュール 1500 において管理される。

【0215】

さらに、メモ리카ード 160 に記録される著作物データについては、まず、音楽データ（コンテンツデータ）自体を暗号化するための共通鍵であるコンテンツキー K_c があり、この共通鍵 K_c により暗号化コンテンツデータが復号（平文化）されるものとする。

【0216】

また、配信サーバ 10 から携帯電話機 600 に向けて、コンテンツキー K_c が配信される場合には、このコンテンツキー K_c は、すくなくとも秘密復号鍵 K_{com} により復号可能なように暗号化されており、メモ리카ード 160 中には、この暗号化コンテンツキー $[K_c]$ K_{com} として格納されているものとする。

【0217】

さらに、著作権の存在するコンテンツデータ D_c は、このコンテンツデータをコンテンツキー K_c で復号化可能な暗号化コンテンツデータ $[D_c]$ K_c としてメモ리카ード 160 に格納されているものとする。

【0218】

〔メモ리카ードの構成〕

図 21 は、図 19 に示したメモ리카ード 160 の構成を説明するための概略ブロック図である。

【0219】

メモ리카ード 160 の構成が、実施の形態 5 のメモ리카ード 150 の構成と異

なる点は、コンテンツキーKcがメモリ1412中においては、暗号化データ[Kc]Kcomとして格納されている点である。

【0220】

メモ리카ード160のその他の部分は、実施の形態5のメモ리카ード150の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【0221】

なお、図21のメモ리카ード160内も、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールTRMに組込まれる構成とすることも可能である。

【0222】

〔再生処理〕

図22は、携帯電話機600内において、メモ리카ード160に保持された暗号化コンテンツデータから、音楽を再生して外部に出力するための再生処理を説明するフローチャートである。

【0223】

図22を参照して、携帯電話機のキーボード1108等からのユーザの指示により、再生リクエストが与えられると（ステップS600）、携帯電話機600の[KPp, Crtf]KPma保持部1560からメモ리카ード160に対してデータ[KPp, Crtf]KPmaが出力される（ステップS602）。

【0224】

メモ리카ード160においては、このデータ[KPp, Crtf]KPmaを復号部1460により復号し、公開暗号化鍵KPpと認証データCrtfとを獲得する（ステップS606）。コントローラ1420は、認証データCrtfに基づいて携帯電話機600の認証を行ない（ステップS606）、携帯電話機600が正規の機器であれば処理をステップS608に移行し、携帯電話機600が正規の機器でない場合、再生のための動作を行わずに処理を終了する（ステップS634）。

【0225】

携帯電話機600が正規の機器である場合、コントローラ1420は、セッションキー発生部1450を制御してセッションキーKs2を発生させる（ステップS608）。コントローラ1420の制御により、このセッションキーKs2を暗号化処理部1452は公開暗号化鍵Kpにより暗号化して暗号化セッションキー[Ks2]Kpを生成し、この暗号化セッションキー[Ks2]Kpを、データバスBS3、端子1202およびメモリインタフェース1200を介して、携帯電話機600に対して送信する（ステップS610）。

【0226】

携帯電話機600では、カード160からの暗号化セッションキー[Ks2]Kpを受信すると、切換え回路1550を介して復号処理部1530が暗号化セッションキー[Ks2]Kpを受けて復号しセッションキーKs2を獲得する（ステップS612）。

【0227】

携帯電話機600においては、セッションキー発生部1552においてセッションキーKs1を生成し（ステップS614）、暗号化処理部1554が、ステップS612において抽出されたセッションキーKs2により、セッションキーKs1を暗号化して暗号化セッションキー[Ks1]Ks2を生成し、データバスBS2を介して、カード160に対して送信する（ステップS616）。

【0228】

メモリカード160は、携帯電話機600により生成された暗号化セッションキー[Ks1]Ks2を受け取り、復号処理部1454においてセッションキーKs2により復号し、セッションキーKs1を抽出する（ステップS618）。

【0229】

続いて、メモリカード160は、メモリ1412から、暗号化コンテンツキー[Kc]Kcomを読出す（ステップS620）。

【0230】

続いて、メモリカード160は、暗号化処理部1456において、抽出したセッションキーKs1により、暗号化コンテンツキー[Kc]Kcomを暗号化し

、暗号化された暗号化コンテンツキー [[Kc] Kcom] Ks1 をデータバス BS3 等を介してデータバス BS2 に与える (ステップ S622)。

【0231】

携帯電話機 600 の復号処理部 1556 は、メモリカード 160 から送信された暗号化された暗号化コンテンツキー [[Kc] Kcom] Ks1 に対してセッションキー Ks1 により復号処理を行なうことにより、暗号化コンテンツキー [Kc] Kcom を取得する (ステップ S624)。

【0232】

さらに、携帯電話機 600 の復号処理部 1572 は、復号処理部 1556 から暗号化コンテンツキー [Kc] Kcom を受け、Kcom 保持部 1570 からのキー Kcom に基づいて、データ [Kc] Kcom の復号処理を行なう (ステップ S626)。

【0233】

復号処理部 1572 が、復号処理によりコンテンツキー Kc を抽出できた場合は (ステップ S628)、処理は次のステップ S630 に進み、抽出できない場合は (ステップ S628)、処理は終了する (ステップ S634)。

【0234】

復号処理部 1572 が復号処理により、コンテンツキー Kc を抽出できた場合は、メモリカード 160 は、暗号化コンテンツデータ [Dc] Kc をメモリ 1412 から読出し、データバス BS3 等を介してデータバス BS2 に与える (ステップ S630)。

【0235】

携帯電話機 600 の復号処理部 1520 は、暗号化コンテンツデータ [Dc] Kc を、抽出されたコンテンツキー Kc により復号処理して平文のコンテンツデータ Dc を生成し、音楽再生部 1508 は、コンテンツデータ Dc を再生して混合部 1510 に与える。デジタルアナログ変換部 1512 は、混合部 1510 からのデータを受け取って変換し、外部に再生された音楽を出力し (ステップ S632)、処理が終了する (ステップ S634)。

【0236】

このような構成とすることで、実施の形態 4 の携帯電話機 400 およびメモリカード 140 の奏する効果と同様に、携帯電話機 600 からのデータ [K P p, C r t f] K P m a に基づいて、メモリカード 160 が認証の結果、正規の機器と判断された携帯電話機 600 とメモリカード 160 の間でしか再生動作が行なわれないため、システムのセキュリティの向上と、著作権者の著作権の保護を図ることが可能となる。

【0237】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【0238】

【発明の効果】

以上説明したとおり、本願発明にかかるデータ再生装置では、正規のユーザがメモリ中に格納したコンテンツデータに対して、第三者が不当に配信データへのアクセスを行なうことが困難な構成となっているので、著作権者および正当なユーザが、無断で行なわれる不当な処理により不利益を被るのを防止することが可能となる。

【図面の簡単な説明】

【図 1】 本発明の情報配信システムの全体構成を概略的に説明するための概念図である。

【図 2】 図 1 に示した携帯電話機 100 の構成を説明するための概略ブロック図である。

【図 3】 携帯電話機 100 内において、暗号化コンテンツデータから音楽を再生するための再生処理を説明するフローチャートである。

【図 4】 本発明の実施の形態 2 の携帯電話機 200 の構成を説明するための概略ブロック図である。

【図 5】 図 4 に示した携帯電話機 200 において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

【図 6】 図 4 に示したメモ리카ード 120 の構成を説明するための概略ブロック図である。

【図 7】 携帯電話機 200 内において、暗号化コンテンツデータから音楽を再生するための再生処理を説明するフローチャートである。

【図 8】 本発明の実施の形態 3 の携帯電話機 300 の構成を説明するための概略ブロック図である。

【図 9】 図 8 に示した携帯電話機 300 において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

【図 10】 図 8 に示したメモ리카ード 130 の構成を説明するための概略ブロック図である。

【図 11】 携帯電話機 300 内において、暗号化コンテンツデータから音楽を再生するための再生処理を説明するフローチャートである。

【図 12】 本発明の実施の形態 4 の携帯電話機 400 の構成を説明するための概略ブロック図である。

【図 13】 図 12 に示した携帯電話機 400 において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

【図 14】 図 12 に示したメモ리카ード 140 の構成を説明するための概略ブロック図である。

【図 15】 メモ리카ード 140 に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明するフローチャートである。

【図 16】 本発明の実施の形態 5 の携帯電話機 500 の構成を説明するための概略ブロック図である。

【図 17】 図 16 に示したメモ리카ード 150 の構成を説明するための概略ブロック図である。

【図 18】 メモ리카ード 150 に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明するフローチャートである。

【図 19】 本発明の実施の形態 6 の携帯電話機 600 の構成を説明するための概略ブロック図である。

【図 20】 図 19 に示した携帯電話機 600 において使用される通信のた

めのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

【図 21】 図 19 に示したメモリカード 160 の構成を説明するための概略ブロック図である。

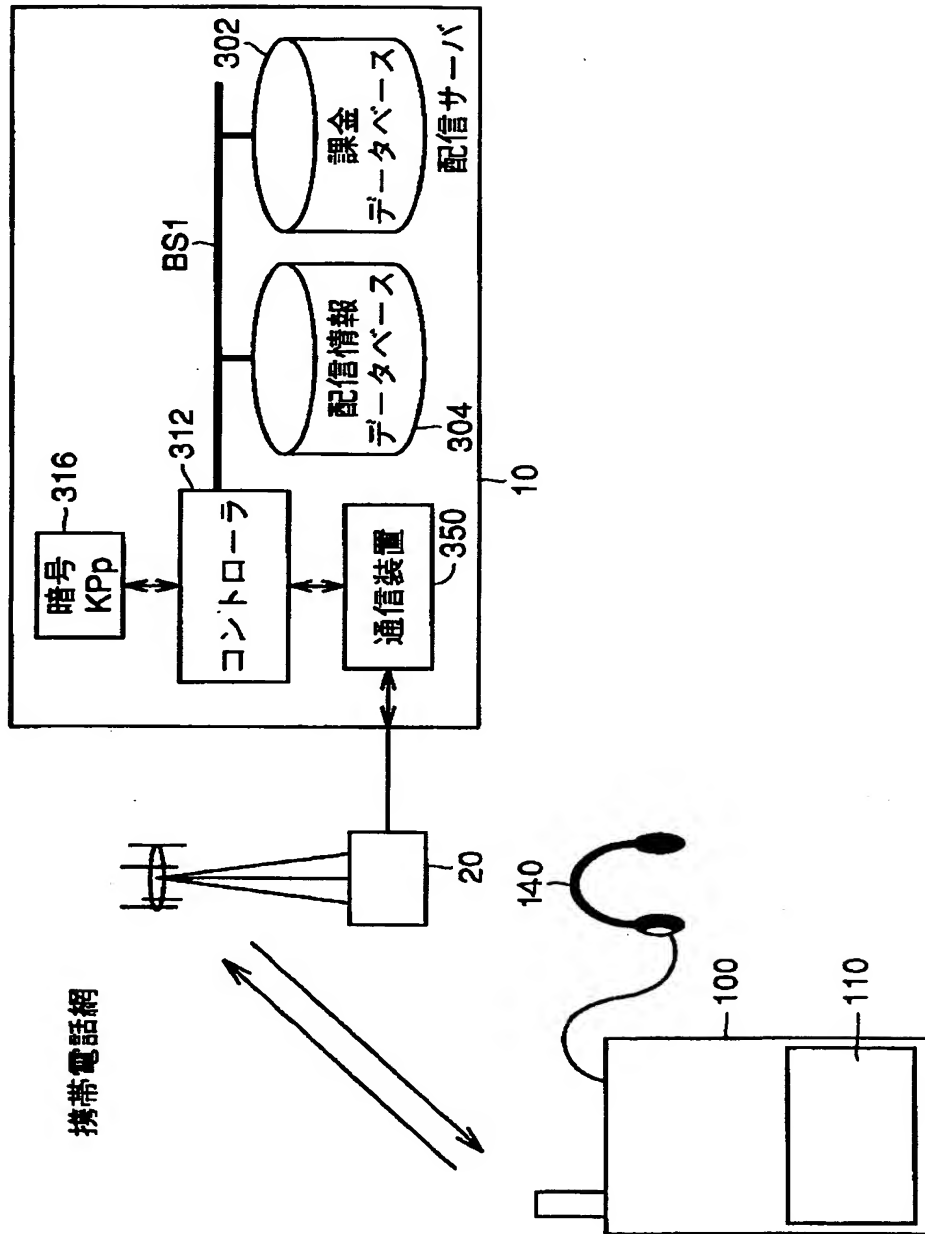
【図 22】 メモリカード 160 に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明するフローチャートである。

【符号の説明】

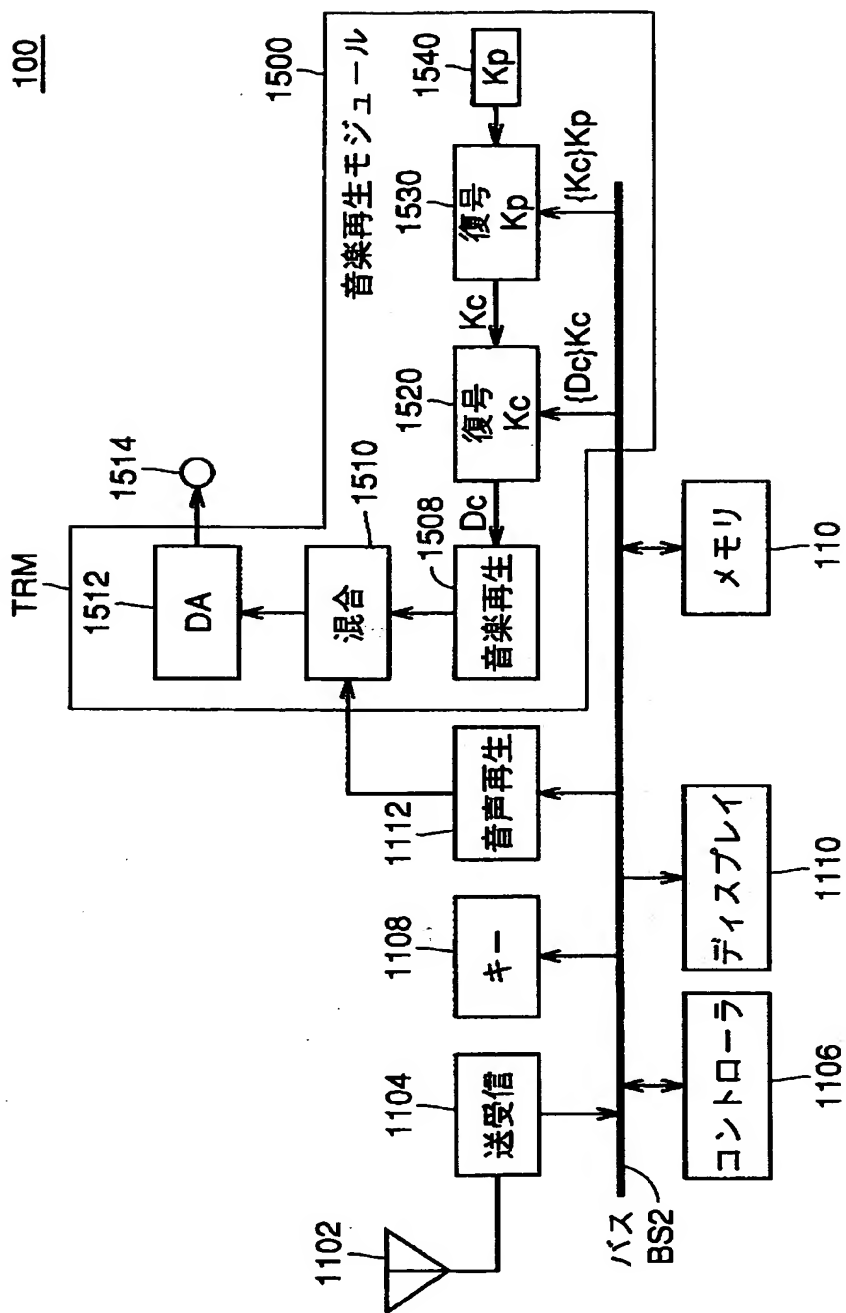
10 配信サーバ、20 配信キャリア、30 音楽サーバ、100, 200, 300, 400, 500, 600 携帯電話機、110, 120, 130, 140, 150, 160 メモリカード、140 ヘッドホン、1102 アンテナ、1104 送受信部、1106 コントローラ、1108 キーボード、1110 ディスプレイ、1112 音声再生部、1200 メモリインタフェース、1401 K P m 保持部、1404 復号処理部、1406 暗号化処理部、1420 コントローラ、1502 セッションキー発生部、1504 暗号化処理部、1506 復号処理部、1508 音楽再生部、1510 混合部、1512 デジタルアナログ変換部、1520, 1530 復号処理部、1540 K p 保持部、1550 切換え回路、1560 [K P p、C r t f] K P m a 保持部、1570 K c o m 保持部、1572 復号処理部。

【書類名】 図面

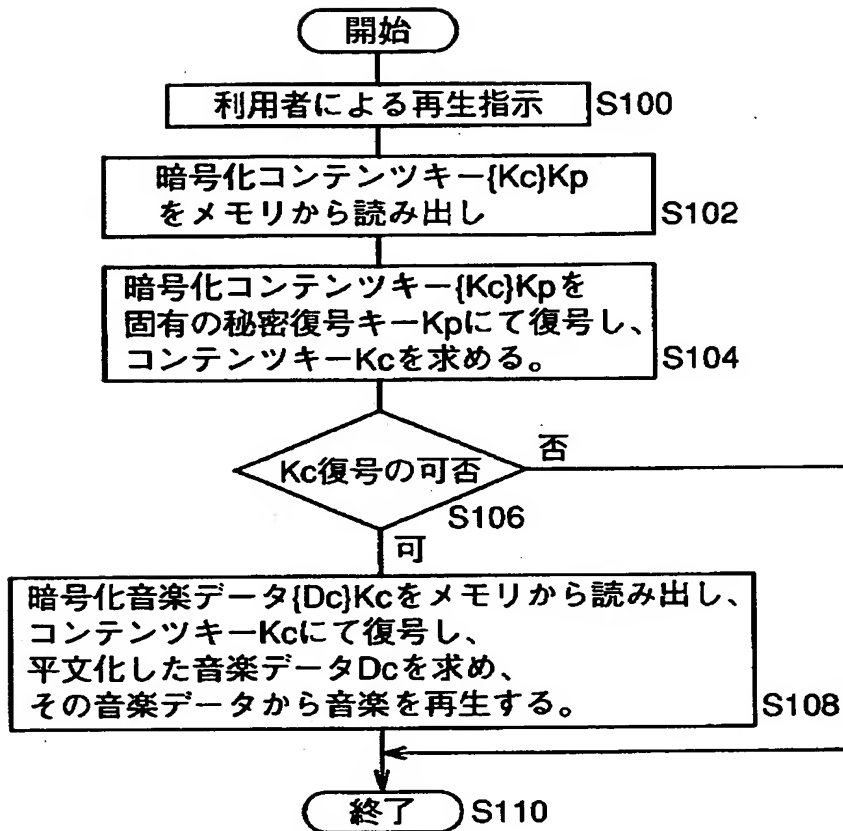
【図 1】



【図 2】

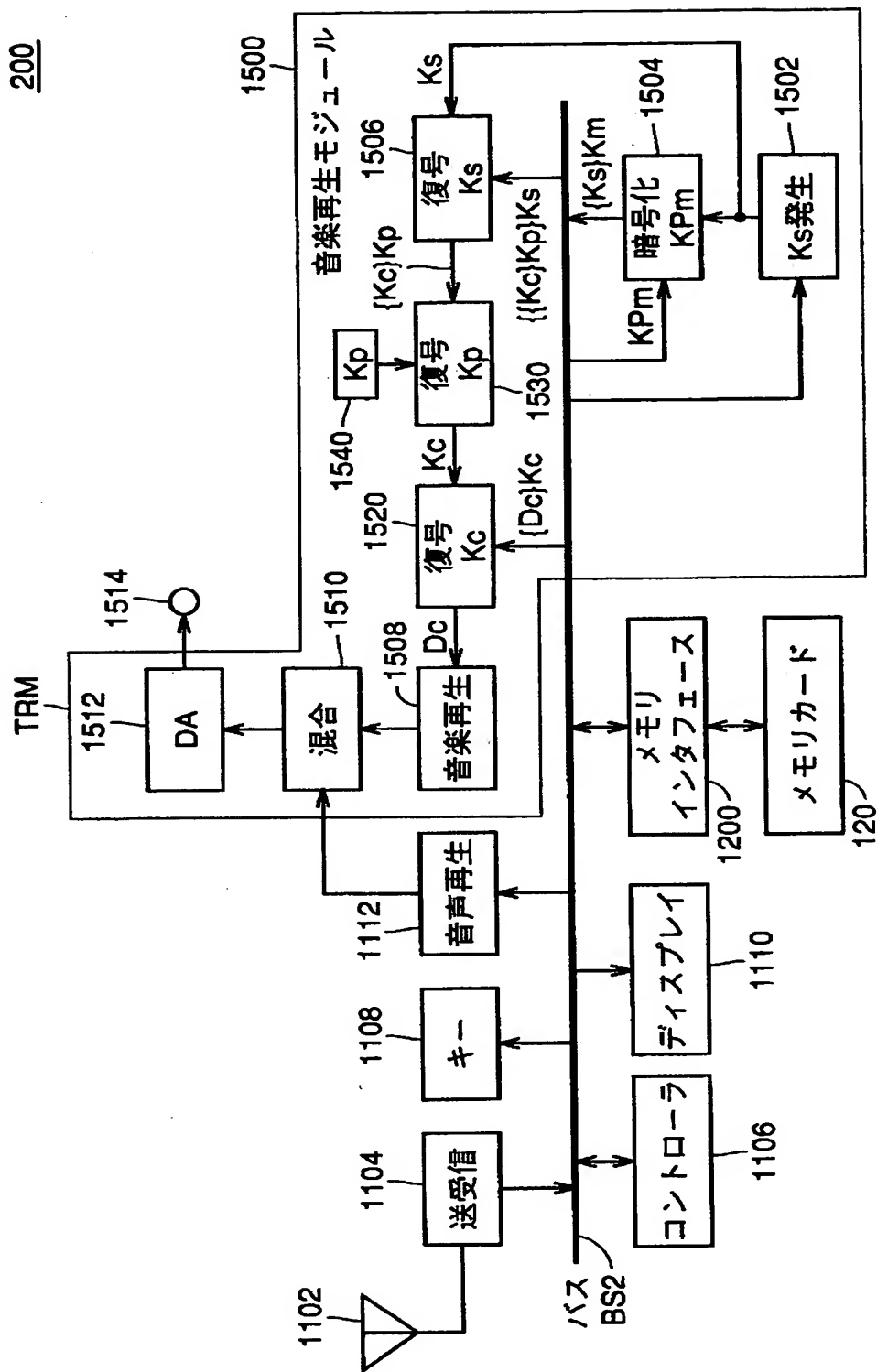


【図 3】



【図 4】

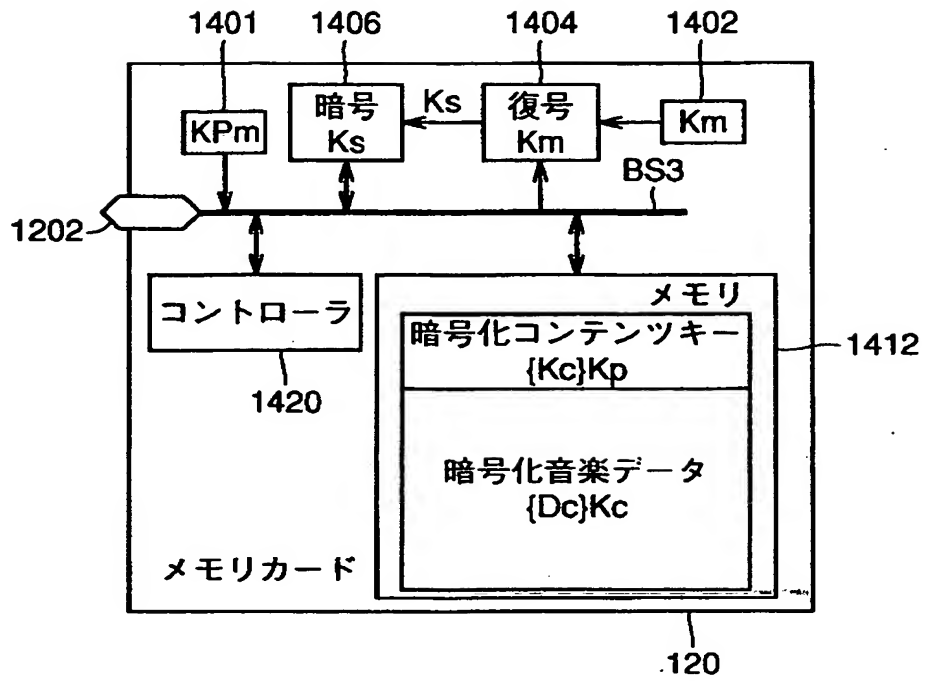
200



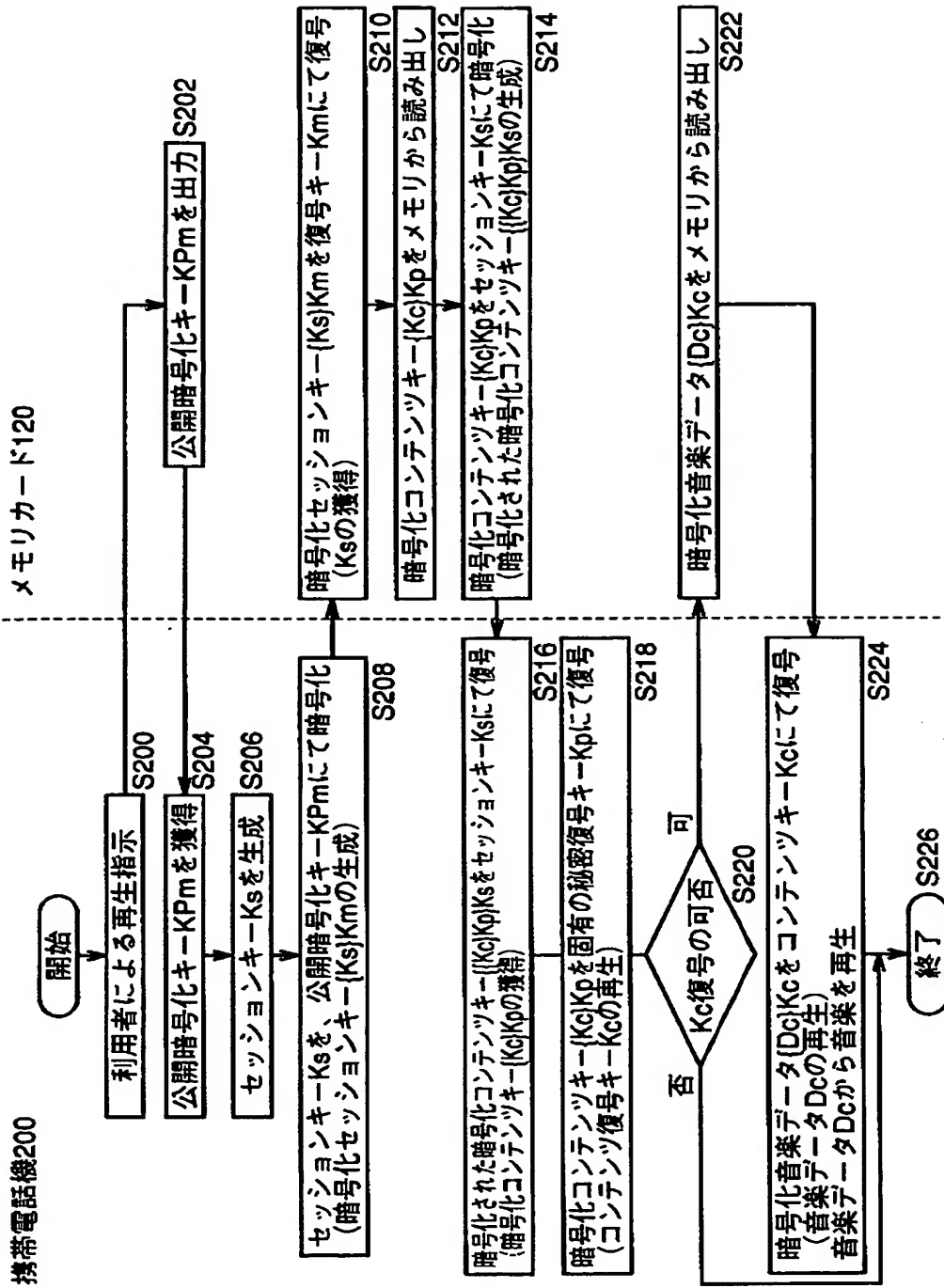
【図 5】

	記号	属性	特性	
メモリカード 管理の鍵	Km	秘密復号鍵		メモリカード毎に異なる
	KPm	公開暗号鍵	Kmと対を成す	KPmで暗号化されたデータは非対称な 復号鍵Kmで復号可能
	Kp	秘密復号鍵	データ再生装置 (携帯電話機) 固有	データ再生装置毎に異なる
音楽再生モジュール 管理の鍵	Ks	共通鍵	セッション固有	メモリと音楽再生モジュール間 のアクセス毎に発生
	KPp	公開暗号鍵	Kpと対を成す (Kcを暗号化)	KPpで暗号化されたデータは非対称な 復号鍵Kpで復号可能
	Kc	共通鍵	コンテンツキー	暗号化コンテンツデータの復号鍵
配信データ	Dc	データ	コンテンツ データ	例：音楽データ

【図 6】

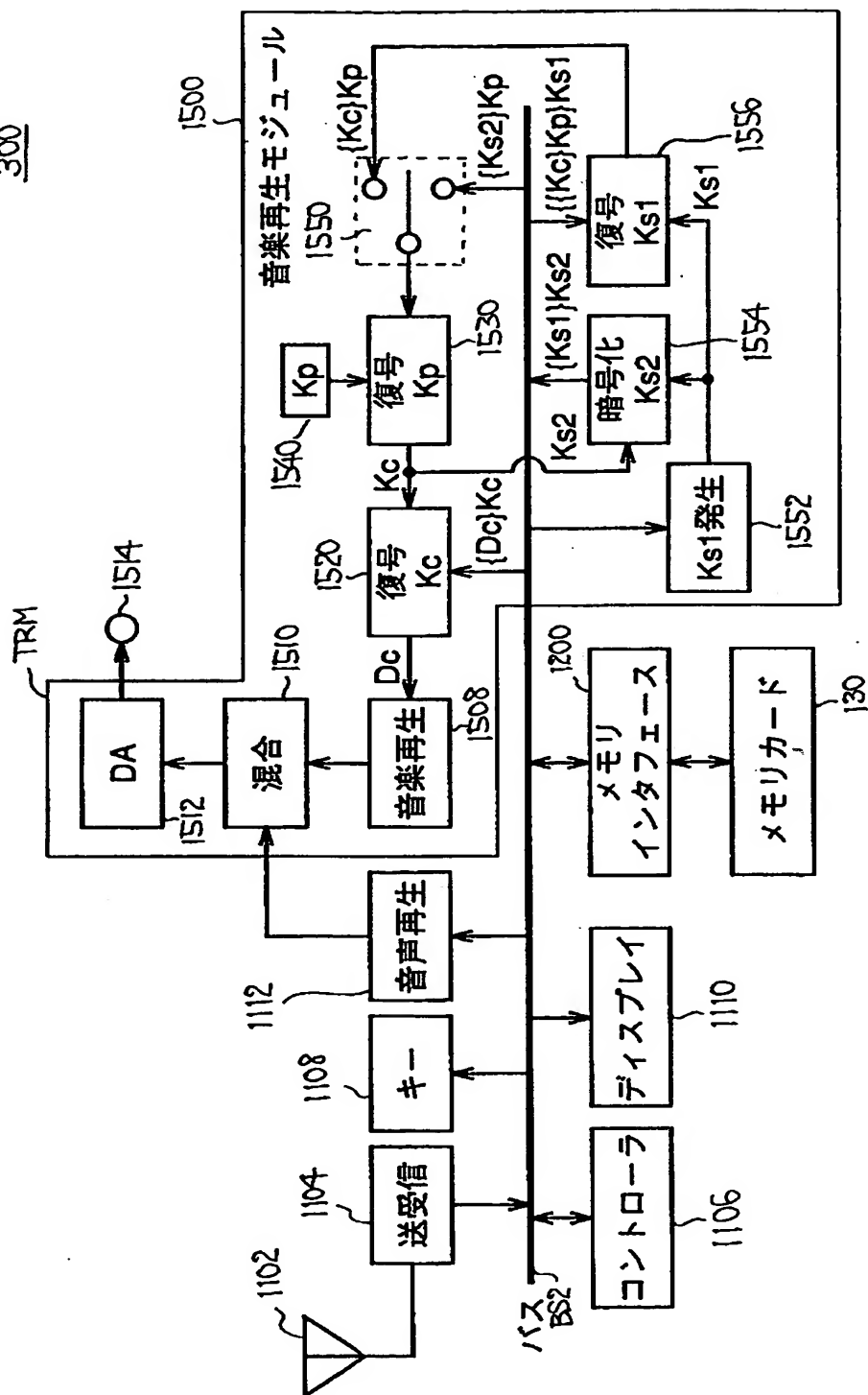


【図 7】



【図 8】

300

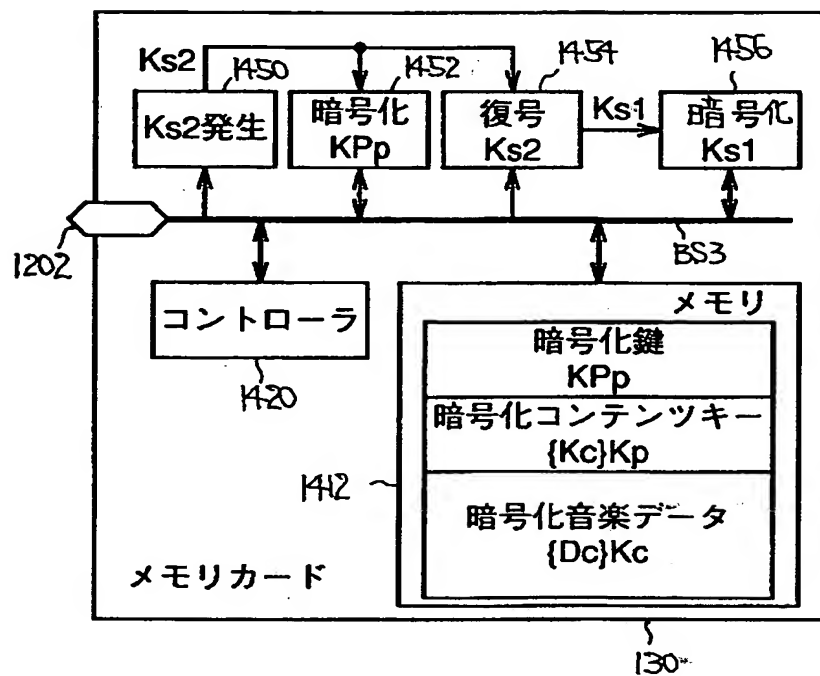


【図 9】

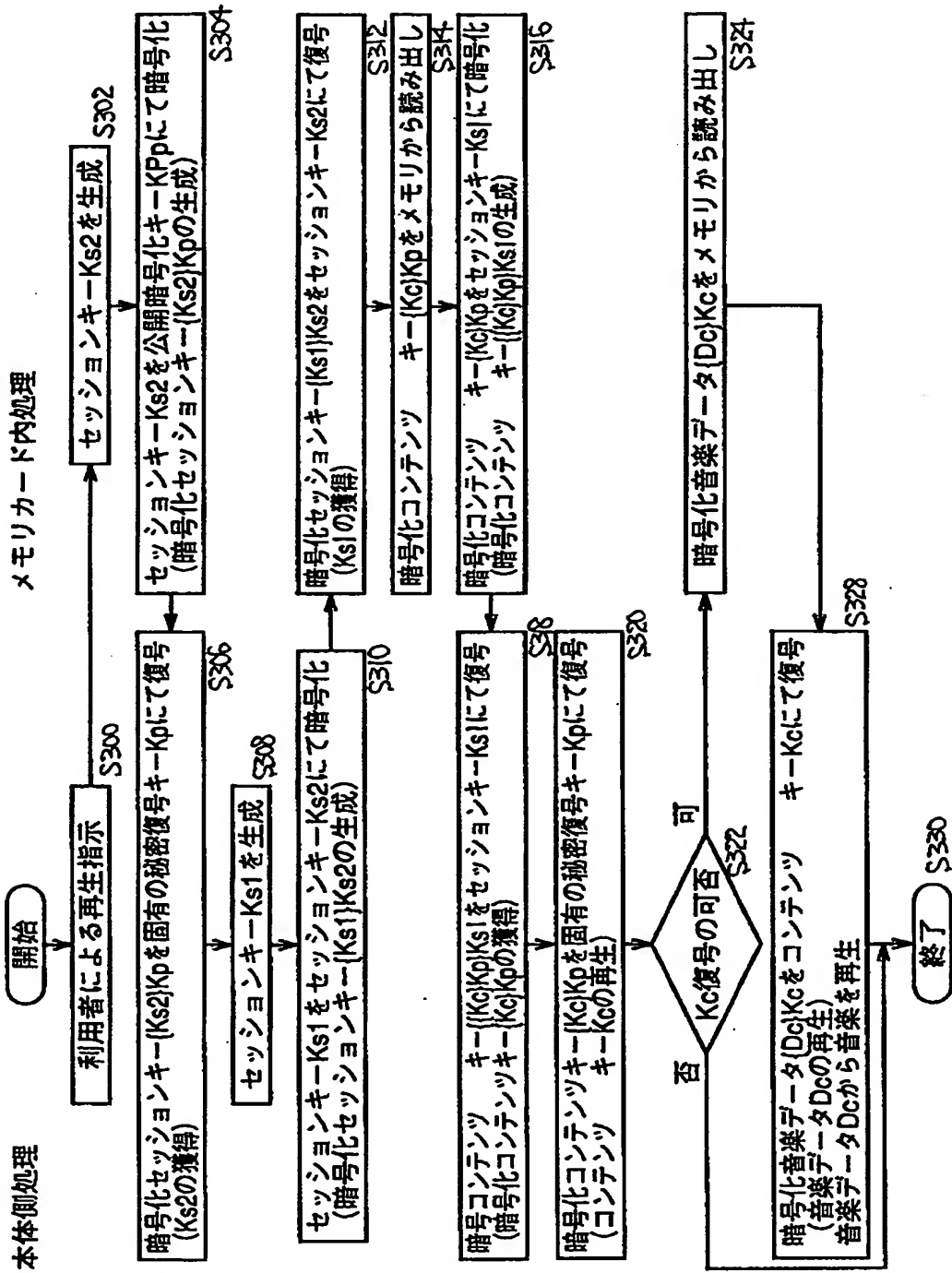
	記号	属性	特性
メモリカード 管理の鍵	Km	秘密復号鍵	メモリカード毎に異なる
	KPm	公開暗号鍵	KPmで暗号化されたデータは非対称な 復号鍵Kmで復号可能
	Ks2	共通鍵	メモリと音楽再生モジュール間 のアクセサス毎に発生
	Kp	秘密復号鍵	データ再生装置毎に異なる (携帯電話機) 固有
音楽再生モジュール 管理の鍵	Ks1	共通鍵	セッション固有
	KPp	公開暗号鍵	KPpで暗号化されたデータは非対称な 復号鍵Kpで復号可能
配信データ	Kc	共通鍵	暗号化コンテンツデータの復号鍵
	Dc	データ	例：音楽データ コンテンツ データ

【図 1 0】

メモ리카ード内の構造

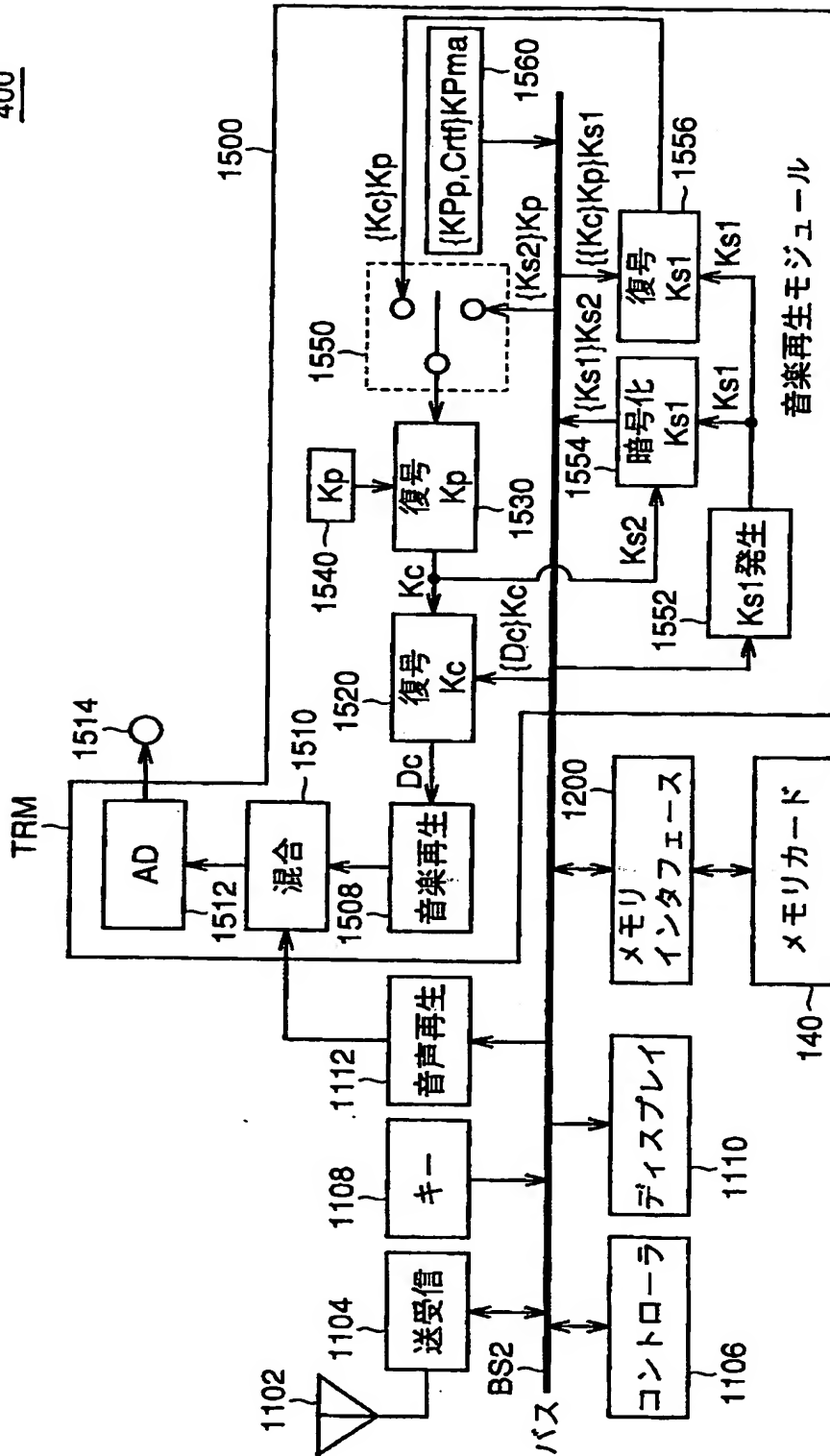


【 図 1 1 】



【図 1 2】

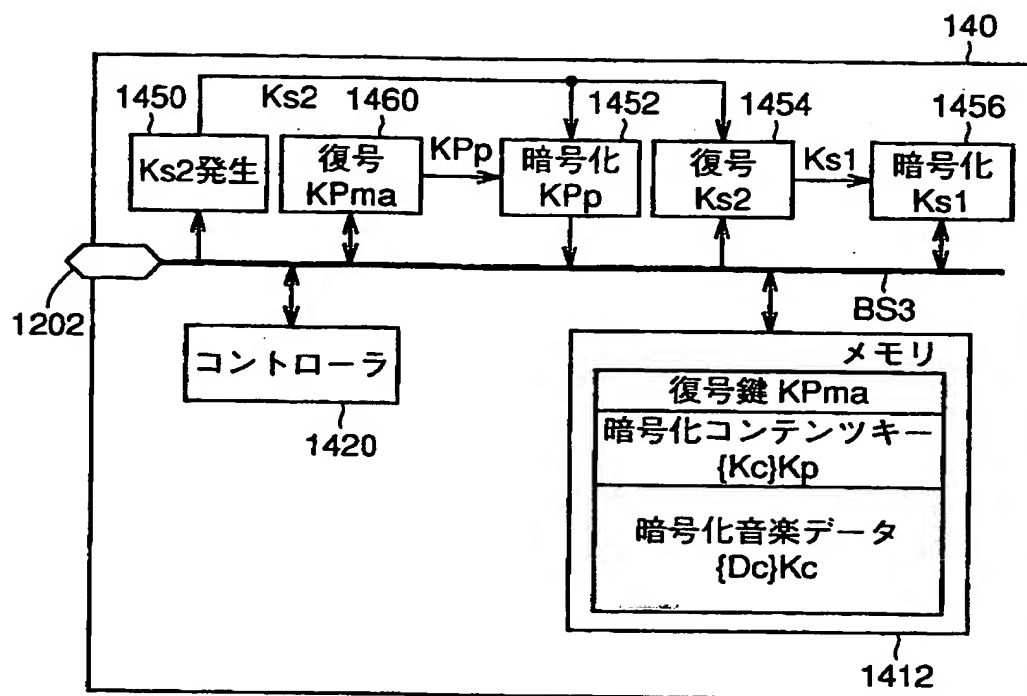
400



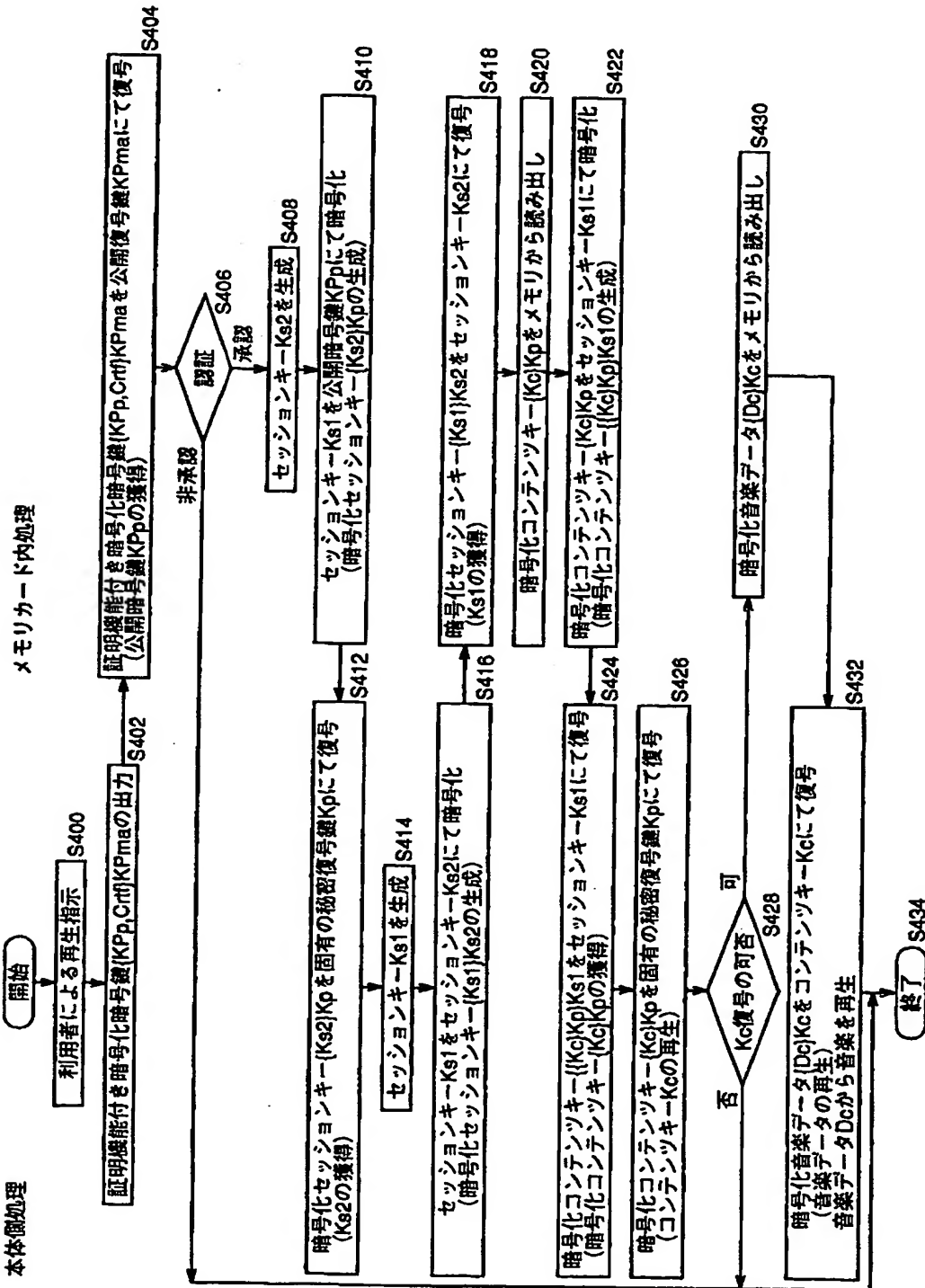
【図 13】

	記号	属性	特性	
			システム共通	{Kp, Crt}Kpmaの復号によってKpの認証を行う機能を有する 認証鍵
メモリカード 管理の鍵	KPma	公開復号鍵	システム共通	
	Ks2	共通鍵	セッションキー	メモリカードと音楽生成モジュール間のアクセス毎に発生
音楽生成 モジュール 管理の鍵	KPp	公開暗号鍵	再生装置のクラス (種類等)固有	データ再生装置毎或いはデータ再生装置の種類によって異なる 非対称な秘密復号鍵Kpにて復号可能
	Kp	秘密復号鍵	再生装置のクラス (種類等)固有	データ再生装置毎或いはデータ再生装置の種類によって異なる 非対称な公開暗号鍵Kpにて暗号化した暗号データを平分化
	Ks1	共通鍵	セッション固有	メモリカードと音楽生成モジュール間のアクセス毎に発生
配信データ	Kc	共通鍵	コンテンツキー	暗号化コンテンツデータの復号鍵
	Dc	データ	コンテンツデータ	例：音楽データ

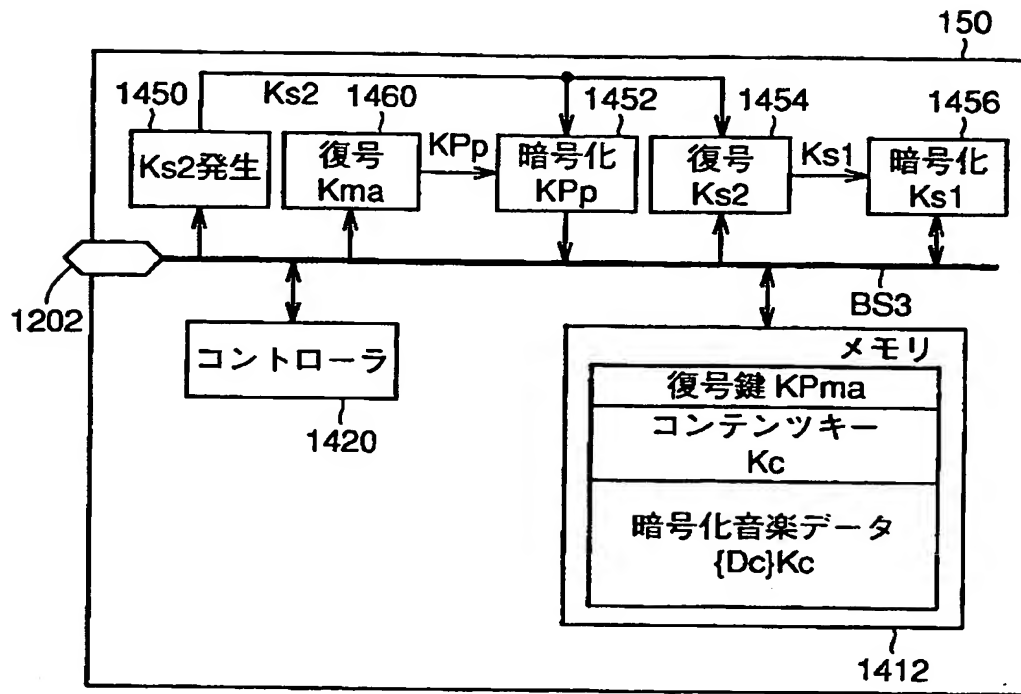
【図 1 4】



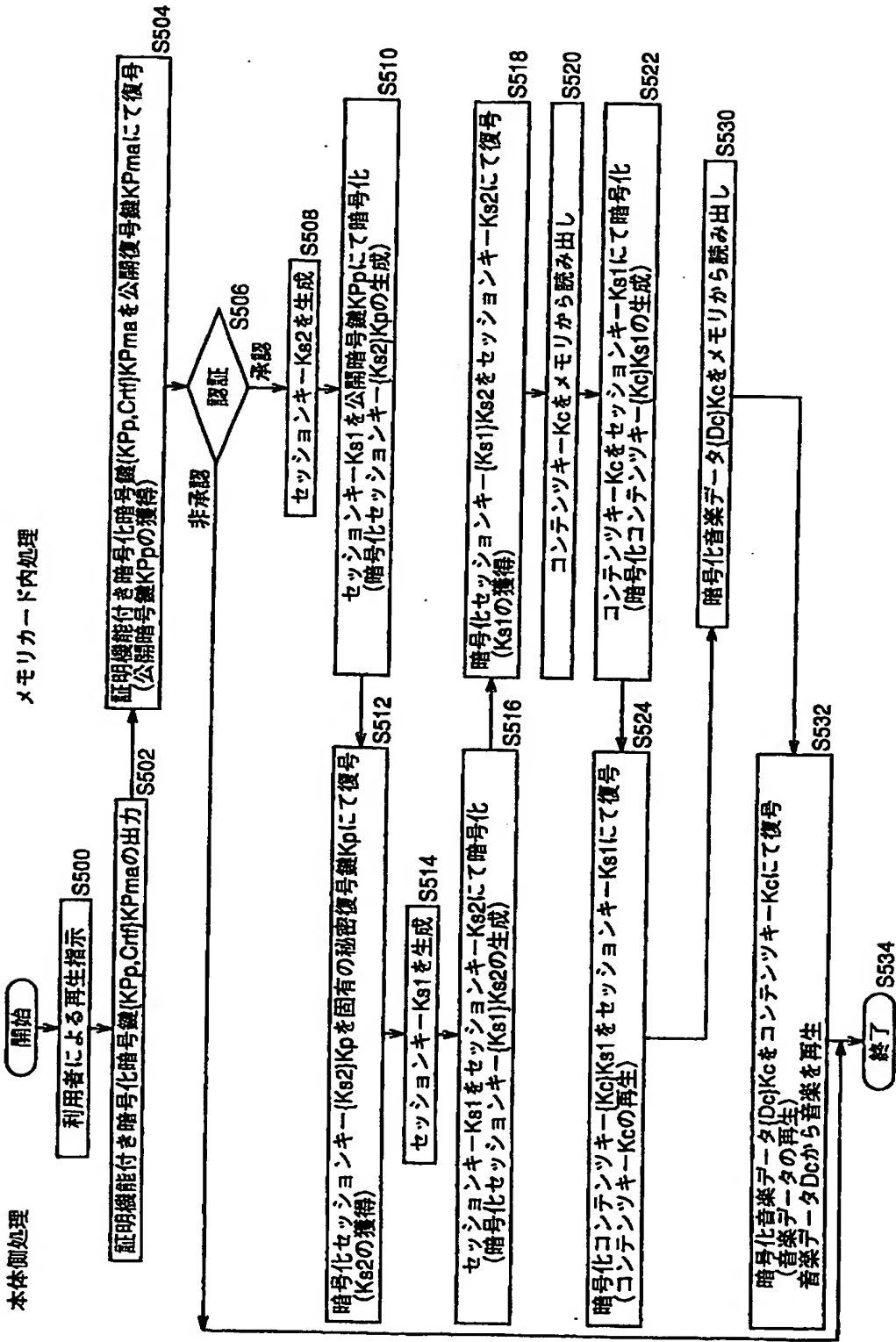
【図 1 5】



【図 1 7】

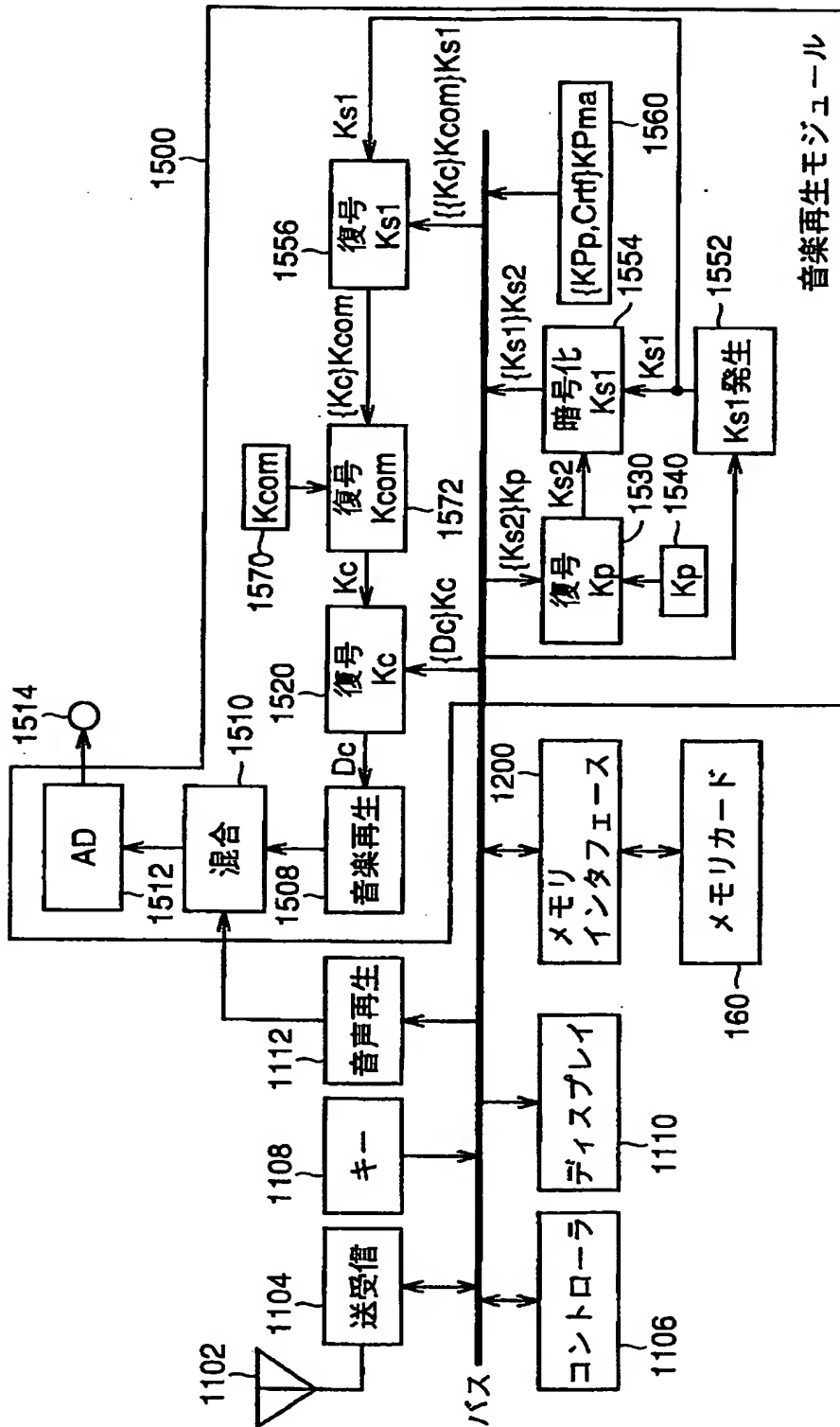


【図 18】



【图 19】

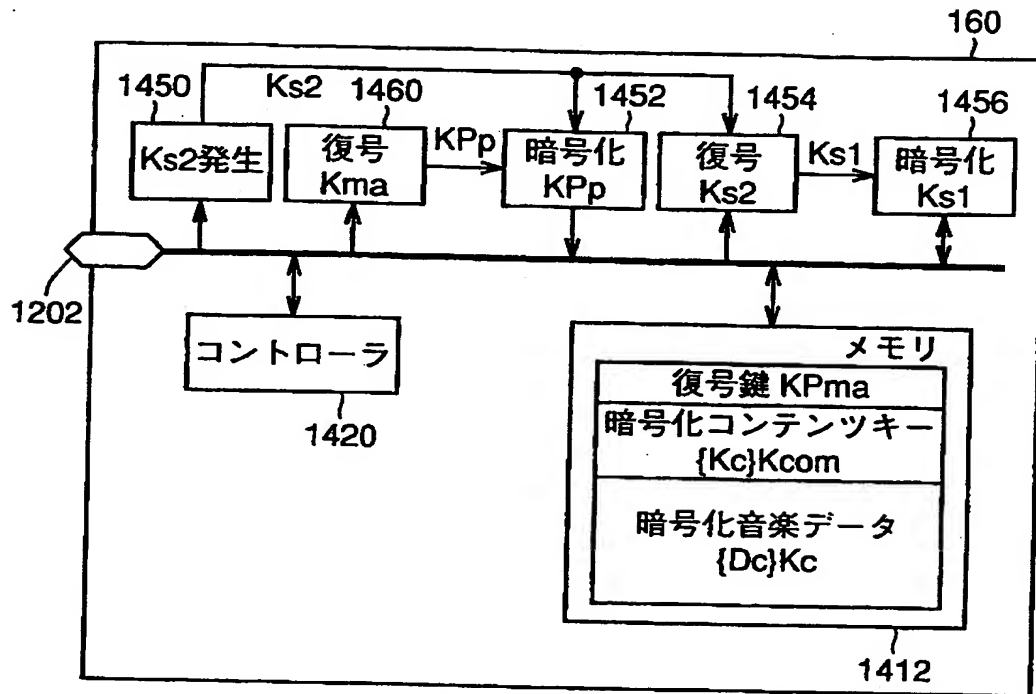
600



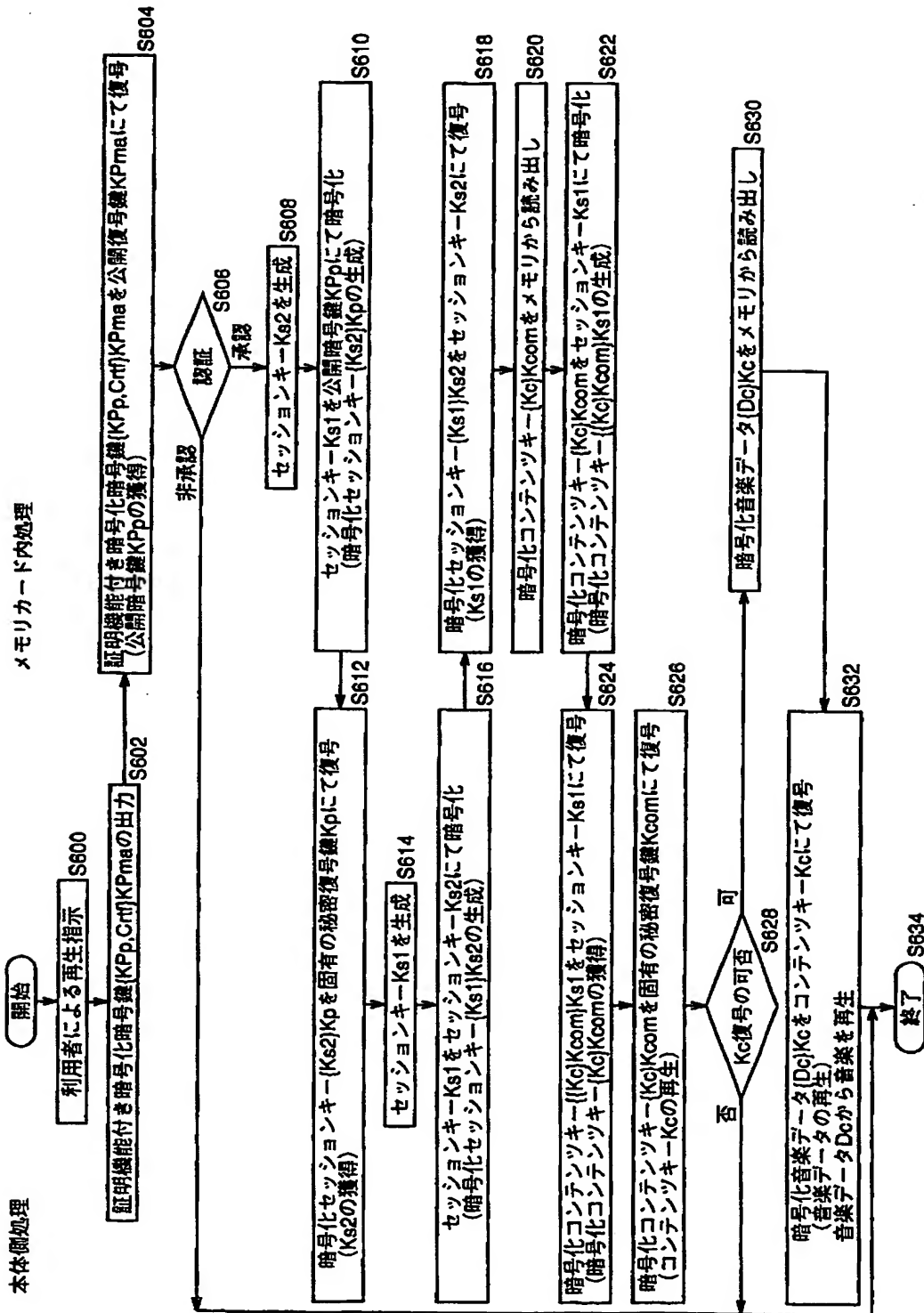
【図 2 0】

	記号	属性	特性	
			システム共通	{Kp}KPmaの復号によってKPpの認証を行う機能を有する認証鍵
メモ리카ード 管理の鍵	KPma	公開復号鍵		
	Ks2	共通鍵	セッションキー	メモ리카ードと音楽生成モジュール艦のアクセス毎に発生
音楽生成 モジュール 管理の鍵	KPp	公開暗号鍵	再生装置のクラス (種類等)固有	データ再生装置毎或いはデータ再生装置の種類によって異なる 非対称な秘密復号鍵Kpにて復号可能
	Kp	秘密復号鍵	再生装置のクラス (種類等)固有	データ再生装置毎或いはデータ再生装置の種類によって異なる 非対称な公開暗号鍵KPpにて暗号化した暗号データを平分化
	Kcom	秘密復号鍵	システム共通	暗号化されたコンテンツキーを復号する
	Ks1	共通鍵	セッション固有	メモ리카ードと音楽生成モジュール艦のアクセス毎に発生
配信データ	Kc	共通鍵	コンテンツキー	暗号化コンテンツデータの復号鍵
	Dc	データ	コンテンツデータ	例：音楽データ

【図 21】



【図 2 2】



【書類名】 要約書

【要約】

【課題】 許可なく著作権物データにアクセスされることを防止することが可能なデータ再生装置を提供する。

【解決手段】 携帯電話機 100 は、配信された暗号化コンテンツデータおよび暗号化コンテンツキーをメモリ 110 に格納する。メモリ 110 から読み出された暗号化コンテンツキーデータは、K_p 保持部 1540 の保持するキーデータ K_p により復号処理部 1530 により復号されて、音楽再生モジュール 1500 に取り込まれる。復号処理部 1520 は、メモリ 110 から読み出した暗号化コンテンツデータを、復号処理部 1530 により抽出されたコンテンツキー K_c により復号して、コンテンツデータ D_c を再生する。

【選択図】 図 2

認定・付加情報

特許出願の番号	平成11年 特許願 第343707号
受付番号	59901178467
書類名	特許願
担当官	塩崎 博子 1606
作成日	平成12年 2月10日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000005223
【住所又は居所】	神奈川県川崎市中原区上小田中4丁目1番1号
【氏名又は名称】	富士通株式会社

【特許出願人】

【識別番号】	000004167
【住所又は居所】	東京都港区赤坂4丁目14番14号
【氏名又は名称】	日本コロムビア株式会社

【特許出願人】

【識別番号】	000001889
【住所又は居所】	大阪府守口市京阪本通2丁目5番5号
【氏名又は名称】	三洋電機株式会社

【代理人】

【識別番号】	100064746
【住所又は居所】	大阪府大阪市北区南森町2丁目1番29号 住友銀行南森町ビル 深見特許事務所
【氏名又は名称】	深見 久郎

【選任した代理人】

【識別番号】	100085132
【住所又は居所】	大阪府大阪市北区南森町2丁目1番29号 住友銀行南森町ビル 深見特許事務所
【氏名又は名称】	森田 俊雄

【選任した代理人】

【識別番号】	100091409
【住所又は居所】	大阪府大阪市北区南森町2-1-29 住友銀行南森町ビル 深見特許事務所
【氏名又は名称】	伊藤 英彦

【選任した代理人】

次頁有

認定・付加情報（続き）

【識別番号】	100096781
【住所又は居所】	大阪府大阪市北区南森町2-1-29 住友銀行 南森町ビル 深見特許事務所
【氏名又は名称】	堀井 豊

出 願 人 履 歴 情 報

識別番号

[000001889]

1. 変更年月日	1993年10月20日
[変更理由]	住所変更
住 所	大阪府守口市京阪本通2丁目5番5号
氏 名	三洋電機株式会社